Tanja Vesterinen

PC:n ja Internetin tietoturva

Opinnäytetyö

Kevät 2010

Tekniikan yksikkö

Tietojenkäsittelyn koulutusohjelma

Digitaalituotanto

Seinäjoen ammattikorkeakoulu
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

SEINÄJOEN AMMATTIKORKEAKOULU

OPINNÄYTETYÖN TIIVISTELMÄ

Koulutusyksikkö: Tekniikka
Koulutusohjelma: Tietojenkäsittely
Suuntautumisvaihtoehto: Digitaalituotanto

Tekijä: Tanja Vesterinen

Työn nimi: PC:n ja Internetin tietoturva

Ohjaaja: Erkki Koponen

Vuosi: 2010 Sivumäärä: 66 Liitteiden lukumäärä: 0

PC:n ja internetin tietoturvauhkien tunnistaminen ja ennaltaehkäisy ovat tietoyhteiskunnassa entistä välttämättömämpiä tietokoneen ja internetin käyttäjille. Internetrikollisuuden kasvaessa uusia haittaohjelmia ja palvelunesto-hyökkäyksiä tehdään enemmän kuin koskaan. Haittaohjelmien historian ja kehityksen tuntemus on hyödyllinen jokaiselle tietoverkkoa käyttävälle henkilölle, jotta he voivat ymmärtää kotikoneilleen tarttuvien haittaohjelmien rakenteen ja toimintatavat sekä osata turvata henkilökohtaiset tietonsa käyttäen hyväkseen oppimaansa tietoa.

Tämän opinnäytetyön tavoitteena on kuvata kirjallisiin lähteisiin perustuen PC:n ja internetin tietoturvauhkia ja niiden torjuntatoimenpiteitä. Opinnäytetyön tuloksista voidaan todeta, että internetiä käyttävien henkilöiden vastuu tietoturvan ja sen uhkien ymmärtämisestä on muodostumassa tärkeimmät tietoverkkojen käyttämisen edellytykset tämän vuosikymmenen edetessä. Inhimillinen tietoturva on pääosassa internetrikollisuuden leviämisessä ja siitä saatavasta taloudellisesta hyödystä. Tietokoneen käytön vastuun edistäminen on tietoverkkojen toiminnan kannalta elintärkeää, sillä ihminen on oman tietoturvansa suurin uhka.

Asiasanat: Tietoturva, tietoturva-uhka, haittaohjelma.

Salaisuus: ei salainen

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Faculty: School of Technology
Degree programme: Data Processing
Specialisation: Digital Media Production

Author/s: Tanja Vesterinen

Title of the thesis: PC and Internet Security

Supervisor(s): Erkki Koponen

Year: 2010 Number of pages: 66 Number of appendices: 0

In today's information society, the ability to recognize personal computer and internet data security threats is more necessary than ever for the internet users and the free use of information networks. In the growing state of internet crime, more new malware and denial of service attacks are made than ever. Knowledge of the history and development of malware is useful for every person who use the information network, in order for them to understand the structure and method of malware and therefore secure their own information security.

The objective of this thesis is to profile PC and internet security threats and their prevention measures based on written sources. The results of the thesis state that the responsibility of using information networks and understanding security threats will become one of the most important conditions of network usage in the following century. Humane computer security is essential when considering the increasing amount of internet crime and the growing economical benefit for the criminals. The responsibility of using computers and information security enhancement is crucial for the function of information networks, because man is the biggest menace for his information security with his own actions and negligence of the vital responsibilities.

Keywords: computer security, computer viruses, malware

SISÄLLYS

SISÄLLYS

KÄYTETYT TERMIT JA LYHENTEET

Mato	*Mato* on Internetin kautta tarttuva, haitallinen ohjelmistokoodi.
Internetrikollisuus	Internetissä tehtävät rikokset, kuten tietojenkalastelu, spam ja huijausviestit.
Hakkeri	Henkilö, joka murtautuu suojattuun tai suojaamattomaan tietoverkkoon.
Kiintolevy	Tietokoneen osa, jossa sijaitsee kaikki tietokoneella oleva tieto.
Looginen pommi	Haittaohjelma, joka kytketään päälle tiettynä päivämääränä tai päivämäärän jälkeen.
Tietoturva-aukko	Tietokoneella sijaitsevan ohjelmiston koodissa sijaitseva haavoittuvaisuus, jota hakkerit voivat käyttää hyväkseen.
Kauko-ohjattu trojan	Trojan, jonka toimintaa ohjataan haittaohjelman tekijän tietokoneelta.
Keylogger	Trojanin muoto, joka kerää omaan loki- tiedostoonsa kaikki näppäimistöllä tehdyt toiminnot.
Loki- tiedosto	Tiedosto, joka sisältää tietoja ohjelmistojen, verkon tai käyttäjän toimista.
Varmenne	Internetsivulla oleva tunniste, jolla voi varmistaa palvelun turvallisuuden.

P2P- ohjelma	Ohjelma, jolla voidaan ladata ja jakaa laittomia sekä laillisia tiedostoja.
Netiketti	Tietoverkon käytön epäviralliset, tietoverkon palveluiden tarjoajien sekä sisällöntuottajien säännöt

KUVIO JA TAULUKKOLUETTELO

1 JOHDANTO

Tietoturva on yksi tietokoneen käyttämisen tärkeimmistä edellytyksistä. Tämän päivän tietoyhteiskunnassa on tärkeää suojata henkilökohtaista tietoa. Internetyhteyksien yleistymisen myötä tavalliselle tietokoneen ja internetin käyttäjälle on muodostunut vastuu tietoturvauhkien ymmärtämisestä, torjunnasta, poistamisesta sekä ennaltaehkäisystä.

Tässä opinnäytetyössä kuvataan, mitä tietoturvauhat ovat ja kuinka käyttäjä omalla käyttäytymisellään parantaa tietoturvan tasoa; miten tietoturvauhat toimivat ja tarttuvat sekä ohjeita tietoturvauhkien poistamiseen ja ennaltaehkäisyyn. Opinnäytetyö sisältää myös ohjeita tietoturvauhkien varalta. Ohjeiden avulla on mahdollista varautua lähivuosina uhkaaviin haittaohjelmiin ja tietomurtoihin sekä parantaa oman tietoturvan tasoa.

Opinnäytetyö sisältää kuusi lukua.
Luku 2 kertoo tietoturvan tärkeydestä ja tietoturvauhkien kehityksestä ensimmäisestä viruksesta nykyisiin tietoturvauhkiin. Luvussa 3 keskitytään tahallisesti tehtyihin tietoturvauhkiin, niiden toimintaan ja ominaisuuksiin. Lisäksi kerrotaan inhimillisistä tietoturvauhkista ja ihmisen oman toiminnan vaikutuksista tietoverkkojen tietoturvaan. Luvuissa 4 ja 5 tutkitaan, miten tietoturvauhkia voi ehkäistä ja millä tavoin tietoturvauhkan voi poistaa tietokoneelta. Luku 6 sisältää johtopäätökset ja vinkit henkilökohtaisen tietoturvan ylläpitämiseksi sekä kertoo tulevaisuuden tietoturvauhista.

2 TIETOTURVA

Tietoturva on tärkeä osa tietoverkkoa ja sen tuoma vapaa maailmanlaajuinen tietoverkko on kallisarvoinen ihmiskunnalle. Ilman tietoturvaa internet ja tietoverkko eivät olisi voineet kehittyä nykyiseen muotoonsa. On hyvä tietää, mitä tietoturva tarkoittaa ja miten tietoturva on kehittynyt nykyiseen muotoonsa, jotta tietoverkkojen käyttäjä voi ottaa vastuuta omista tietoturvaa heikentävistä teoistaan. Tässä luvussa keskitytään tietoturvan tärkeyteen, sen peruspilareihin, historiaan ja kehityskulkuun tähän päivään saakka.

2.1 Tietoturvan tärkeys

Mitä olisi internetin käyttö ilman tietoturvaa?
Voiko *tietoverkko*a käyttää ilman tietoturvan tuomaa suojaa?

Vastaus on hyvin yksinkertainen: tämän päivän tietoverkossa tietoturva on välttämätön tietoverkon toiminnan kannalta. Ilman tietoturvaa, tietoverkon käyttö on vaarallista ja edesvastuutonta. Se on niin tärkeä, että ilman tietoturvaa ei olisi olemassa nykyisen kaltaista maailmanlaajuista tietoverkkoa.

Tietoturvallisuus koskettaa kaikkia ihmisiä ja ihmisten tekemiä toimintoja internetissä, kotona ja yrityksissä. Luottamuksellisuus, eheys sekä käytettävyys ovat tietoturvan tärkeimmät peruspilarit. Luottamuksellisuuden ansiosta tietoverkossa oleva tieto on vain niiden henkilöiden käytössä, jotka omaavat siihen tarvittavan käyttö-oikeuden. Eheys ja käytettävyys mahdollistavat tiedon todenmukaisuuden sekä tietojen saatavuuden oikeaan aikaan. (Tampereen Yliopisto, 2009)

Tietoturva takaa ja suojaa henkilöiden ja prosessien toiminnan turvallisuuden. Siihen vaikuttavat tietoverkon käyttäjien ja tietoverkkoa varten tarkoitettujen laitteiden kanssa tekemisissä olevat prosessit. Nämä tietoturvauhkiksi nimitetyt prosessit ovat uhka tietoverkkoa käyttävillle henkilöille, heidän tietokoneilleen ja niiden sisältämälle henkilökohtaiselle tiedolle sekä koko maailmanlaajuisen tietoverkon ra-

kenteelle. Suurin syy tietoturvauhkiin on ihminen. Ihminen tekee virheitä, rikkoo sääntöjä, on välinpitämätön, ylihuolehtivainen, ilkeä, sinisilmäinen, pahantahtoinen, osaamaton – kaikkea mistä tietoturvariskit johtuvat ja minkä vuoksi tietoturvauhkia ylipäätään on olemassa. Ihminen tekee inhimillisiä virheitä ja saattaa toimia tahallisesti luoden uusia tietoturvauhkia tai vahingossa levittää haittaohjelmia muille tietoverkkoa käyttäville henkilöille. (Rosendahl 2010.)
Tietoturvan avulla ihmisen aiheuttamia riskejä voidaan estää, mutta vastuu tietoturvasta on itse tietoverkkoa käyttävällä yksilöllä. Jos tietoverkon käyttäjät ymmärtäisivät toimintojensa riskit ja tietoverkon käytön vastuun, tietoturvauhkia olisi helpompaa ehkäistä, eikä *internetrikollisuus* olisi kovin suuri ongelma ja uhka yleiselle tietoturvalle.

Tietoturvan tietoinen laiminlyönti on vaarallista tietoverkkojen toiminnalle maailmanlaajuisesti. Se voi aiheuttaa yritysten toiminnan sekä henkilöiden yksityisyyden vaarantumisen, tuhota yksityisiä tietoverkkoja tai muuttaa tietoverkon käyttökelvottomaksi. Tietoturvan laiminlyönti on suurin tunnettu tietoturvauhka, joka edistää haittaohjelmien leviämistä ja uusien tietoturvauhkien kehitystä ja syntyä. Tämän suurimman tietoturvauhkan minimoimiseen on ryhdytty toimiin monissa maissa onnistuneesti, mutta työ inhimillisen tietoturvan edistämiseksi ei koskaan lopu. Tietoverkoissa käydään jatkuvaa sotaa internetrikollisuutta vastaan ja mitä edistyneemmäksi vihollisen aseet muuttuvat, sitä vahvempia keinoja on keksittävä niiden torjumiseen. (Sapronov 2010.)

Internetrikollisuuden määrän kasvaessa ihmisten oma vastuu tietoturvasta on lisääntynyt ja vastuun vuoksi tietoturvan tärkeyttä olisi opetettava jokaiselle tietokoneenkäyttäjälle iästä ja taustasta riippumatta. Tämä opetus on tietoturvan ja tietoverkkojen tulevaisuuden näkökulmasta elintärkeää, sillä vastuunsa ymmärtävä internetin käyttäjä on aina yksi askel eteenpäin kohti turvallisempaa tietoverkkoa.

Tietoturvakoulutusta on lisätty jo useisiin peruskouluihin ja oppilaitoksiin, mutta tietoverkon iäkkäämmät käyttäjät jäävät usein ilman tietoa tietoturvan tärkeydestä ja sen tuomasta henkilökohtaisesta turvasta. Suomen valtakunnallinen tietoturvaviikko edistää tietoturvan tärkeyden sanomaa koko Suomessa erilaisilla tapahtumilla

ja oppitunneilla. Tietoturvaviikkoa pidetään myös yli 60 maassa Suomen lisäksi (Viestintävirasto 19.01.2010). Kunnilla, kaupungeilla ja erikokoisilla yrityksillä on myös omia tietoturvapäiviä, jotka antavat tietoa tietoturvan tehtävistä ja sen tuomasta suojasta. Internetistä löytyy myös tietoturvaoppaita jokaiselle tietoverkkoa käyttävälle henkilölle. Koskaan ei ole liian myöhäistä oppia tietoturvan tärkeydestä ja oman tietokoneen suojaamisesta tietoturvauhkia vastaan ja materiaalia siitä löytyy helposti internetistä. (Tietoturvakoulu 2008.)

Yksi tietoturvan laiminlyönti voi johtaa peruuttamattomaan tuhoon jopa valtakunnallisesti. ”*Haittaohjelmien levittäjät voivat halutessaan uhata jopa valtion turvallisuutta. Virossa kaksi vuotta sitten tapahtuneet patsasmellakat ja niihin liittynyt tietoverkkosabotaasi osoitti, että pahimmillaan verkkoiskut voivat lamauttaa koko yhteiskunnan toiminnan”. (Kivioja 2009, 35.)*

Inhimillisten uhkatekijöiden karsiminen auttaa suuresti maailmanlaajuiseen taisteluun tietoturvan suojaamiseksi, mutta taistelu tahallisesti tehtyjä uhkatekijöitä vastaan laajenee eri tekniikoilla seuraavina vuosina ja niitä varten joudutaan kehittämään uusia tapoja tietoturvauhkien torjumiseksi. Tietoturva ei ole kuitenkaan koskaan valmis. Se on prosessi joka kehittyy jatkuvasti ja jota on ylläpidettävä tietoverkon käytön vapauden ja toiminnan turvaamiseksi. (Rosendahl 2010.)

2.2 Tahallisten tietoturvauhkien, sekä tietoturvan historia ja kehittyminen

Vuonna 1969 internetin edeltäjän tietoverkon kehitys oli vasta alkamaisillaan. ArpaNet-niminen tietoverkko tehtiin ohjelmien etäkäyttöä varten ja sitä suunnitellessa tietoturva ei ollut tekijöiden päällimäisenä huolenaiheena. Tietoverkossa oli valmistuessaan monia turvaheikkouksia ja se herätti pian huomiota Yhdysvaltain hallituksessa. Vuonna 1970 Yhdysvaltain puolustusministeriö julkaisi raportin, jossa keskityttiin tietolaitteiden fyysiseen turvallisuuteen sekä datan, käyttäjien ja infrastruktuurin suojaamiseen. Tämä tutkimus toimi suuntaa antavana tietoturvan tutkinnalle ja kehitykselle, ollen pohjana nykypäivän tietoturvan suojaamiselle. (Tietoturvan historia ja tausta, 2010, 8.)

Ensimmäinen *virus*, Creeper, oli kokeellinen itsensä kopioiva ohjelma, joka kehitettiin vuonna 1971. Creeper käytti ArpaNetiä leviämisväylänään. Se saastutti DEC PDP-10 -tietokoneita ja koodillaan sai saastutetuille tietokoneiden näytöille tekstin *"I'm the creeper, catch me if you can!"*. Virus puhdistettiin The Reaper -ohjelmalla, joka kehitettiin ainoastaan Creeper-viruksen poistamista varten. The Reaper oli alkeellinen virustorjuntaohjelma, jota viruksen tavoin levitettiin tietoverkossa tietokoneisiin, mutta ohjelman päämäärä oli hyväksyttävä siitä saadun hyödyn vuoksi. (Reisinger 2010.)

1970-luvulla tietoverkkoa varten kehitettiin monia uudistuksia, kuten Telnet-etäkäyttö, FTP (File Transition Protocol), Ethernet, TCP (Transmission Control Protocol) ja IP (Internet Protocol). Nämä suuret tekniset uudistukset mahdollistivat tietokoneiden ja internetin käyttöönoton yrityksissä ja kotona 1980-luvun alusta lähtien. Vuonna 1980 markkinoille tuotiin uusi tapa tallentaa tiedostoja, asentaa ohjelmia ja siirtää tietoa tietokoneelta toiselle, 3.5-tuuman levyke tuli yleisesti käyttöön kodeissa ja yrityksissä, mikä johti internetin historian ensimmäiseen vapaasti leviävään virukseen. (Tietoturvan historia ja tausta, 2010, 8-9.)

Ensimmäinen vapaasti levinnyt virusohjelma Rother J, kirjoitettiin vuonna 1981. Se tartutti Apple DOS 3.3 -käyttöjärjestelmiä leviten 3.5 tuumaisen pelilevykkeen kautta. Virus kirjoitettiin vitsinä tietokonepeliin ja pelin viidennenkymmenen käynnistyskerran jälkeen se saastutti tietokoneen Elk Cloner- viruksella. Levykkeistä tuli yksi tietoturvan suurimmista uhkatekijöistä, koska ne saastuttivat koneen helposti levykeasemaan jäätyään. Tietokoneet yrittivät käyttää levykeaseman levyä käynnistyslevynään ja näin virukset tarttuivat helposti tietokoneiden käynnistyssektoreille. Levykkeiden käytön vähennyttyä käynnistyssektorivirukset katosivat miltei kokonaan. (Resick 2010.)

Varsinainen internet syntyi vuonna 1982, kun ArpaNet-tietoverkko hajotettiin kahteen osaan. Arpanet jaettiin sotilas- ja siviiliosiin, jolloin tietoverkon sisältö ja turvallisuus muuttui täysin. Lopputuloksesta syntyi nykyisin käytetty maailmanlaajuinen tietoverkko, jonka käyttäjäkunta kasvoi räjähdysmäisesti käyttöliittymien, puhelinyhteyksien sekä graafisten selainten yleistyessä. Käyttäjämäärän nopea

kasvu siirsi hakkereiden kiinnostuksen puhelinverkoista tietoverkkoihin. Seuraavina vuosina perustettiin useita *hakkeri*ryhmiä eri maissa. Koska tietoverkkoja koskevia lakeja ei ollut vielä kehitetty, hakkerit saivat tehdä tietoturvarikoksia kaksi vuotta ilman minkäänlaisia seuraamuksia. Vuonna 1986 Yhdysvaltain kongressi hyväksyi lakiehdotuksen Computer Fraud and Abuse Act, joka teki tietomurroista ja haittaohjelmien teosta sekä levityksestä rikoksen. Jo samana vuonna viisi hakkeria pidätettiin vakavista tietomurroista, ja taistelu tahallisesti tehtyjä tietoturvauhkia vastaan alkoi vahvoin ottein. (Tietoturvan historia ja tausta, 2010, 10.)

Vuosi 1986 toi mukanaan myös ensimmäiset PC-virukset. Brain-, Virdem-, Burger- ja Rush Hour -virukset eivät levinneet laajalti, mutta olivat esimerkkeinä seuraavina vuosina ilmestyneille viruksille. Uudet vuoden 1987 virukset Jerusalem, Lehighm, Stoned ja Vienna olivat uusia ja erilaisia viruksia. Jerusalem oli ensimmäinen muistiin tarttunut haittaohjelma, josta tehtiin seuraavina vuosina kolme uutta versiota. Stoned-virus tartutti tietokoneen käynnistysosion, joka antoi jokaiselle tietokoneen käynnistyskerralle mahdollisuuden tekstille: *”Your PC is now Stoned!”.* Stoned-viruksesta tehtiin useita eri versioita, joista tuli 1990- luvun alkupuoliskolla erittäin yleisiä ja laajalti levinneitä haittaohjelmia. (Wells 1996.)

Uusi tiedon tallennus- ja jakoväline, CD-R-levyke, aloitti tietokonealan valloituksen vuonna 1988. 3.5 tuuman levykkeet saivat näin rinnalleen uuden tiedonsiirtovälineen, joka antoi haittaohjelmien tekijöille uusia mahdollisuuksia ohjelmien levittämiselle. Samana vuonna luotiin ensimmäinen virus, joka oli tehty Brain-viruksen poistoa varten. Den Zuk -viruksesta tehtiin kaksi eri versiota. Näitä viruksia sanottiin anti-virus-viruksiksi ominaisuuksiensa vuoksi. Kyseinen virus ei tuhonnut tai haitannut tietokoneen käyttöä muulla tavalla, kuin puhdistamalla Brain-viruksen. Tämä oli ensimmäisiä tietoturvaohjelmia, joka puhdisti tarttuneen tietoturvauhkan tietokoneen *kiintolevy*ltä. (Tietoturvan historia ja tausta 2010.)

Vuoden 1989 puolivälissä tunnettiin jo 30 virusta, joskin harvat tietokoneet olivat joutuneet näiden tietoturvauhkien kohteeksi. Esimerkiksi Jerusalem-virusta vastaan oli alettu kehittämään jo ensimmäistä virustorjuntaohjelmaa, joka tunnisti viruksia ja *trojan*eita heurestisesti. Tämä virustorjuntaohjelma ei kuitenkaan yleisty-

nyt, mutta oli esimakua tuleville virustorjuntaohjelmille ja valonpilkahdus tietoturvan synkentyväksi muuttuvassa tulevaisuuden näkymässä. (Wells 1996.)

Loppuvuonna 1989 virukset DataCrime, Jerusalem ja Dark Avenger saivat median kiinnostumaan ja hätääntymään mahdollisista tietoturvauhkista. DataCrime- ja Jerusalem-virukset saivat medialta huikeasti näkyvyyttä niiden mahdollisten ominaisuuksiensa vuoksi. Nämä kaksi virusta olivat ensimmäiset virukset, jotka ohjelmoitiin aktivoitumaan tiettynä päivämääränä tai päivämäärän jälkeen. DataCrime ja Jerusalem olivat niinsanottuja *loogisia pommeja*. Ne sisälsivät aikakytkimen, jonka aktivoituessa virukset aktivoivat koodinsa tietokoneen kiintolevyllä. Virusten leviäminen ja tartunnan seuraukset eivät lopulta vastanneet median odotuksia ja tartuntojen vakavuus oli yliarvioitua. (Wells 1996.)

1990-luvulle siirryttäessä tietokoneiden ja tietoverkon käyttäjien määrä alkoi nousta erittäin nopeasti. Internetistä saatava tieto ja sieltä löytyvät palvelut alkoivat kiinnostaa uusia tietokoneiden käyttäjiä sekä internetrikollisia. IP-huijaus, verkon nuuskinta ja tietojärjestelmiin tunkeutuminen olivat rikollisten erityisen kiinnostuksen kohteena. Näitä tietoturvauhkia varten luotiin uutena teknisenä ratkaisuna palomuuri. (Tietoturvan historia ja tausta 2010, 11.)

1990-vuoden lopulla virustorjuntaohjelmistoja oli saatavilla jo 18 kappaletta eri tietoturvayrityksiltä, yksi ohjelmistoja tuottavista menestyneistä yrityksistä on Symantec McAfee. 1991 virustorjuntamarkkinoille tuotiin uusi ohjelmisto: Norton AntiVirus, jota myytiin maailmanlaajuisesti. Vuonna 1992 virustorjuntaohjelmistojen kirjo oli jo hyvin laaja, vaikka itse viruksia oli löydetty ja tehty hyvin vähän. Monet yritykset arvoivat virusten määrän lisääntyvän liiankin nopeasti ja laajensivat toimintaansa, johtaen lopulta monien tietoturvayritysten konkursseihin. (Wells 1996.)

ArpaNet-verkko lopetettiin 90-luvun alussa kokonaan ja pian internetiä ryhdyttiin käyttämään myös kaupallisissa tarkoituksissa. Sähköpostia käyttävien henkilöiden määrä moninkertaistui ja jokaiselle annettiin mahdollisuus luoda oma sähköpostitilinsä. Verkkopankit ja sähköinen kaupankäynti laajensivat tietoverkon käyttöä uusiin ulottuvuuksiin ja valitettavasti avasivat samalla oven uusille kehittyneemmille

tietoturvauhkille. Ensimmäinen verkkopankin kautta tapahtunut pankkiryöstö tehtiin jo vuonna 1994, jonka jälkeen verkkopankkien tietoturvaan oli pakko kiinnittää enemmän huomiota ja kehittää uusia tietoturvaratkaisuja tietoturvan säilyttämiseksi. (Tietoturvan historia ja tausta 2010, 11.)

Windows-käyttöjärjestelmän ensimmäinen tietokonevirus ilmestyi 1992-luvun loppupuolella. WinVer 1.4 tartutti exe-päätteisiä sovellustiedostoja ja levisi muihin tietokoneella sijaitseviin exe-tiedostoihin. Vuonna 1993 tunnettiin jo 100 erilaista tietokonevirusta, ja liikkeellä oli vielä paljon tuntemattomia tietoturvauhkia. Helpotusta ei tuonut vuonna 1994 yleistyneet CD-levyt, joilla asennettiin tietokoneille ohjelmia, pelejä ja siirrettiin tiedostoja koneelta toiselle. Tiedonsiirto tällä uudella välineellä levitti jo tunnettuja tietokoneviruksia laajemmalle koti- ja yritysverkoissa. (Wells 1996.)

1990-luvun puolivälistä lähtien makrovirukset yleistyivät huimasti Windows 95 -käyttöjärjestelmän mukana tulleen Microsoft Word -ohjelman avulla. Windows 95 käytti ohjelmissaan WordBASIC -kieltä, jolla haittaohjelmien tekijät ryhtyivät kirjoittamaan uusia, makroviruksiksi nimettyjä tietoturvauhkia. Makrovirukset tarttuivat kaikkiin käyttöjärjestelmiin joilla pystyi käyttämään Microsoft Word -tekstinkäsittelyohjelmaa. Vuosikymmenen lopulla Outlook Express -sähköpostiohjelma ja Internet Explorer -internetselain toimivat yleisimpinä haittaohjelmien leviämisväylinä. (Wells 1996.)

Uusi vuosituhat alkoi tietoturvan näkökulmasta hyvin rauhallisesti, mutta Y2K-uhan väistyttyä, toukokuussa 2000, uusi sähköpostimato ILOVEYOU, tarttui internetissä ennennäkemättömän nopeasti ja aiheuttaen pohjoisamerikkalaisille yrityksille yli 5.5 miljardin dollarin vahingot. Madot yleistyvät pian, ja 2001 vuonna madot Sadmind, Sircam, Code Red 1 & 2, Nimda ja Klez laskivat tietoturvan tasoa ja nostivat haittaohjelmien tartuntamäärää maailmanlaajuisesti. Sähköpostin mukana levinneet tietoturvauhkat kasvattivat määräänsä nopeasti ja tarttuivat räjähdysmäisesti miljooniin tietokoneisiin kodeissa ja yrityksissä. 2000-lukua voidaan kutsua matojen ja trojaneiden vuosikymmeneksi, niiden suuren lukumäärän ja tartuntojen yleisyyden vuoksi. Vaarallisimmiksi viime vuosikymmenen tietoturvauhkista

voidaan nostaa esiin madot Conficker, ILOVEYOU, MyDoom, Sasser ja Storm. (Strickland 2010.)

2000-luvulla uudet käyttöjärjestelmät ja ohjelmistoversiot jättivät rikollisille hyödynnettäviksi useita *tietoturva-aukko*ja. Uusilla käyttöjärjestelmillä on ollut valtava vaikutus uusien tietoturvauhkien syntymiselle ja tietoturvan kehitykselle. Mitä edistyneemmäksi tietokoneiden käyttöliittymät muuttuvat, sitä edistyneempiä tietoturvauhkista tehdään. Näitä edistyneitä tietoturvauhkia vastaan on tehty monia tietokoneen eri osa-alueita suojaavia virustorjuntaohjelmia. Virustorjuntaohjelmistoista on tullut kukoistava miljoonabisnes, johon ovat ottaneet osaa myös internetrikolliset omilla huijausvirustorjuntaohjelmistoillaan.

Jo 23 vuotta jatkunut PC haittaohjelmien esiintyminen jatkuu vahvempana kuin koskaan uusilla kehittyneillä tavoilla. Uudet nopeasti käyttäjiä keräävät ohjelmat ja palvelut ovat nyt erittäin alttiita tietoturvauhkille ja rikollisten hyökkäyksille. Tietoturvauhat ovat kehittyneet valtavasti viimeisen kymmenen vuoden aikana. Ne tarttuvat yhä useampiin tiedostomuotoihin, ovat monimutkaisempia, vaikeasti huomattavia sekä poistettavia, aiheuttavat enemmän tuhoa, tarttuvat yhä useammista lähteistä ja ovat entistä häiritsevämpiä.

Tietoturvan suojelemiseksi joudutaan jatkuvasti kehittämään uusia teknisiä menetelmiä. Tietoturva on aina ollut internetrikollisia yhden askeleen jäljessä. Tietoturvan ja haittaohjelmien tulevaisuutta ei voi ennustaa kovin tarkasti, tietoturva kehittyy sitä mukaa kuin sen uhkaajatkin kehittyvät. Vuonna 1986 tehdyn Computer Fraud and Abuse Act -lain ansiosta tietoverkon käyttö haitallisiin tarkoituksiin on rikos, ja ilman tätä lakia tietoverkot eivät olisi kehittyneet ja levinneet nykyiseen maailmanlaajuiseen käyttöön.

3 TIETOTURVAN UHKATEKIJÄT

Tietoturvauhkat vaikuttavat tietoyhteiskunnan toimintaan ja tietoverkkojen käyttöön joka päivä, joka tunti, joka minuutti ja joka sekunti. Mutta miten nykyajan tietoturvauhkat toimivat ja miten niitä torjutaan tässä tietoverkkojen hallitsemassa maailmassa?

Tässä luvussa syvennytään tietoturvauhkien toimintaan, rakenteeseen ja erilaisiin tietoturvauhkien tyyppeihin, kuten virusten erilaisiin muotoihin sekä muihin tunnettuihin tietoturvauhkiin. Virusten rakenteen ja toiminnan ymmärrys syventää tietokoneen peruskäyttäjän tietämystä tietoturvauhkien toiminnasta ja toimintatavoista. Nykyisin yleisimmät virusten muodot eli trojan -virukset ovat tärkeimpiä tunnistaa ja ymmärtää. Myös matojen ja muiden haittaohjelmien tuntemus on hyväksi jokaiselle tietokoneen käyttäjälle, jotta niitä pystytään torjumaan tehokkaasti ja oikeilla teknisillä sekä inhimillisillä menetelmillä.

Kaikkien tietoturvauhkien lähtökohtana on itse tietokoneen käyttäjä. Inhimilliset tietoturvauhkat ovat tietoverkon käyttäjän omia virheitä joko tietokoneen käytössä tai omassa asenteessaan. Asenteen tai tiedon puutteen vuoksi tapahtuvat tietoturvan laiminlyönnit ovat syy tietoturvan nykyisen tilan heikentymiselle. Kaikki tietoverkkoa käyttävän henkilön omat virheet on lopulta helposti korjattavissa, eikä ihmisen vastuuta tietoverkon käytössä kannata aliarvioida.

3.1 Virusten rakenne ja toiminta

Tietokonevirukset ovat pieniä ohjelmia, jotka ovat tehty leviämään tietokoneesta toiseen aiheuttaen haitallisia seurauksia tietokoneen järjestelmälle tai sen käyttäjälle. Virukset voivat tehdä itsestään toimivan kopion ja kasvattaa lukumääränsä koneen sisällä ennalta-arvattomiin lukemiin. Virukset sekoitetaan usein trojaneihin, matoihin sekä mainos- ja vakoiluohjelmiin. Kyseiset ohjelmat eivät ole kuitenkaan tavallisia viruksia, koska niiltä puuttuu kyky tehdä itsestään kopioita, eivätkä välttämättä aiheuta yhtä vakavia seurauksia tarttuessaan.

Tietokoneviruksia on kahta eri tyyppiä. Yksi virustyypeistä on muistissa pysymätön ja toimii etsien isäntäkoneita tartuttaen niihin haittaohjelman. Virus toimii etsintä- ja monistusmoduuleilla, joiden avulla se etsii isäntäkoneen ja tarttuu siihen joko nopeasti tai hitaasti tarttuvana muotona. Tässä vaiheessa viruksen tehtävänä on ainoastaan levittää itsestään kopioita kiintolevyn eri kansioihin. Etsintämoduuli etsii tartutettavia tiedostoja ja kansioita. (Pcguide 2001.)

Toinen virustyyppi on muistissa pysyvä eikä etsi isäntäkoneita, vaan lataa itsensä tietokoneen muistiin käynnistyessään. Virus pysyy aktiivisena tietokoneessa tartuttaen ohjelmia ja käyttöjärjestelmän tiedostoja. Muistissa toimiva virus ei käytä etsintämoduulia toiminnassaan, vaan monistusmoduuli asentuu suoraan käyttöjärjestelmän muistiin. Monistusmoduuli toimii silloin kun sovellus (tiedostomuoto .exe tai .com) avataan. Se tarttuu avattuun ohjelmaan ja jatkaa tarttumistaan muihin käyttöjärjestelmässä avattaviin sovelluksiin. Muistissa toimivia ja toimimattomia viruksia on kahta eri kategoriaa: nopeat ja hitaat tartuttajat. (Computer Hope 2010.)

Nopeasti tarttuvat virukset yrittävät tarttua lyhyessä ajassa niin moneen tiedostoon kuin mahdollista. Nämä virukset jäävät virustorjuntaohjelmistoilta helposti huomaamatta, sillä ne tarttuvat käyttöjärjestelmän isäntätiedostoihin ja muuttavat virustorjuntaohjelmiston toimintaa täysin päinvastaiseksi. Virustorjuntaohjelma voi virustartunnan jälkeen tartuttaa jokaisen tarkistamansa tiedoston tällä nopeasti leviävällä viruksella. Nopeiden viruksien heikkoutena on korkea huomattavuus, koska virus hidastaa tietokoneen toimintaa ja herättää virustorjuntaohjelmiston huomion epämääräisillä toiminnoillaan. Hitaat virukset tartuttavat isäntätiedostoja satunnaisesti ja yrittävät herättää toiminnallaan mahdollisimman vähän huomiota. Hidas tartuntatapa on suotuisa virustorjuntaohjelman toiminnalle. Hitaasti leviävän viruksen voi saada nopeasti puhdistettua, sillä se ei leviä tärkeisiin tiedostoihin kovinkaan nopeasti. (Pcsecurityalert.com. 2010.)

Kun nopea tai hidas virus tarttuu tiedostoon, se pyrkii pitämään eron tartutetun ja puhtaan tiedoston välillä hyvin pienenä. Tämän saavuttaakseen se ei muuta tiedoston viimeisintä muokkauspäivämäärää tai tiedoston kokoa, sillä käyttäjä huomaa näiden ominaisuuksien muuttuneen helposti resurssienhallinnan kautta.

Virustorjuntaohjelmistot etsivät haittaohjelmia tietokoneen kiintolevyltä ja löytävät viruksen tartutettuihin tiedostoihin viruksen kirjoittaman koodin eli virustunnisteen avulla. (Pcsecurityalert.com. 2010.)

Tietokoneviruksia esiintyy siis muistin varaavina ja varaamattomina sekä hitaana ja nopeana leviämistyyppinä. Viruksella on lisäksi neljää eri tartuntatyyppiä: makro- , komentojono, tiedosto- ja käynnistyslohkovirukset. (Norton from symantec 2006.)

Makrovirukset tarttuvat tietokoneisiin vain niistä ohjelmista, jotka käyttävät Word-BASIC -makrokieltä. Makrokieltä käyttäviä ohjelmia ei ole montaa - vain Microsoft Office -paketin tekstinkäsittelyohjelma Word sekä laskentataulukko-ohjelma Excel ovat yleisyytensä vuoksi saaneet ongelmikseen makrovirukset. Tunnettu Melissa-virus (1999), käytti makrovirusta levitäkseen. Se oli tarttunut LIST.DOC- nimiseen sähköpostiliitteeseen ja lähetti itsensä viidellekymmenelle tallennetulle sähköposti-osoitteelle. Virus käytti hyväkseen sähköpostiohjelma Outlookia ja sen tapaa avata uudet sähköpostit ja niiden liitteet automaattisesti ilman käyttäjän suostumusta. Microsoft Excel sai myös oman vastineensa Melissa-viruksesta. Papavirus toimi ja tarttui samalla tavoin kuin Melissa, mutta se levisi vain Excel- tiedostojen kautta tietokoneen käyttöjärjestelmään. (Kuivanen 2003.)

Komentojonovirukset käyttävät käyttöjärjestelmän komentojonoja tartuttaakseen tietokoneen käyttöjärjestelmän. Ennen käyttöjärjestelmien yleistymistä komentojono-virukset kirjoitettiin MS-DOS- ja UNIX-komentojonoilla. Windows-käyttöjärjes-telmät käyttävät toiminnassaan Visual Basic Scripting (VBS) -kieltä, jolla on tehty useita komentojonoviruksia. Tunnetuin komentojonoja käyttävä virus oli touko-kuussa 2000 laajallle levinnyt VBS.Love-Letter. Se oli sähköpostivirus, joka kirjoi-tettiin tällä käyttöjärjestelmälle tärkeällä VBS -kielellä ja jonka avulla virus pystyi tarttumaan käyttöjärjestelmään huomaamattomasti ja tehokkaasti. VBS- komento-jonoviruksia tavataan nykyään hyvin harvoin, eivätkä ne aiheuta vakavia seurauk-sia tietokoneen käytölle tai henkilökohtaiselle tiedolle. (Helenius 2004.)

Tiedostovirukset tartuttavat tietokoneita .exe- ja .com-tiedostotyypillä olevia tiedos-

toja. Saastunut ohjelma tarttuu tietokoneelle vasta, kun sovellustiedosto avataan asennusta tai käyttöä varten. Tiedostossa sijaitseva ohjelmakoodi tunkeutuu keskusmuistiin ja keskusmuistin kautta tarkkailee muiden ohjelmien käyttöä tarkoituksenaan tartuttaa kaikki käytössä olevat ohjelmatiedostot. Tiedostovirukset voivat olla vaarallisia tai vaarattomia, riippuen tekijän käyttötarkoituksesta. Harmittomat tiedostovirukset eivät sotke tietokoneen käyttöä ja tartuta itseään eteenpäin, mutta vaaralliset virukset voivat johtaa BIOS-järjestelmän täydelliseen korruptoitumiseen. Vaaralliset tiedostovirukset tuhoavat usein myös tietokoneen kiintolevyllä sijaitsevia käyttöjärjestelmälle tärkeitä ja vähemmän tärkeitä tiedostoja. Tiedostovirukset ovat nykyisin hyvin harvinaisia virustorjuntaohjelmien tehokkuuden ansiosta. (Kuivanen 2003.)

Kaikki yllämainitut virukset voivat levitä Windows-, Mac- ja Linux-käyttöjärjestelmällä toimiviin tietokoneisiin, moniin matkapuhelinmerkkeihin ja autojen ajo-tietokoneisiin. Viruksia on eniten Windows-käyttöjärjestelmällä toimivissa tietokoneissa, mutta Mac-tietokoneiden yleistyessä myös niiden tietoturvauhkien määrä on kasvanut ja tulee olemaan kasvusuhdanteessa jatkossakin. Myös Applen tuotteet iPhone ja iPod ovat saaneet omat viruksensa, kuten myös Nokian yleisimmät Symbian-käyttöjärjestelmällä toimivat matkapuhelimet.

Virustartunnan voi saada kaikista internetistä ladatuista laillisista ja laittomista tiedostoista. Viruksia tarttuu myös CD- ja DVD-levyistä, USB-muistitikuista, ulkoisista kiintolevyistä sekä Bluetooth-yhteyden kautta toisesta tartutetusta laitteesta, kuten tietokoneesta tai matkapuhelimesta. Virukset tarttuvat helpoiten sähköpostien liitetiedostoiden tai erilaisten keskustelu- ja tiedostojenjako-ohjelmien kautta. Ne voivat naamioida itsensä liitetiedostoissa kuviksi, tervehdyskorteiksi sekä ääni- että videotiedostoiksi. Yleisesti virukset leviävät Microsoft Office -ohjelman tekstitiedostojen, doc-päätteisten tekstien kautta, joihin on asetettu tiedoston avatessa tarttuva makrovirus. Viruksia on kehitetty myös Adobe Acrobat ohjelman pdf-tiedostoihin, joita internetin käyttäjät ovat tähän asti pitäneet erittäin turvallisina. (Pcsecurityalert.com. 2010.)

Virus voi korruptoida, poistaa ja muuttaa tietokoneella sijaitsevia tiedostoja, käyt-

tää sähköpostiohjelmaa levittämään haittaohjelmia muihin tietokoneisiin tallennettujen sähköpostiosoitteiden avulla sekä kaapata tietoverkon tai tietoverkkoja kokonaan omaan käyttöönsä haittaohjelmien levitämiseksi. Pahimmillaan virus voi tyhjentää tietokoneen kiintolevyn kokonaan, kadottaen ja muuttaen kaikki kiintolevyllä sijaitsevat tiedostot palauttamattomaan muotoon. Monet virukset ja haittaohjelmat sisältävät helposti huomattavia oireita, mutta useat tartunnat voivat jäädä huomaamatta kokonaan, aiheuttaen tartutettuun tietokoneeseen salaa enemmän vaurioita. Virustartunnan huomaa helposti tietokoneen toimintojen ja internetin hidastumisena, käyttöjärjestelmän toimintojen muutoksina, kiintolevyn itsestään täyttymisenä, selaimen kaappauksena, uutena taustakuvana sekä muilla näkyvillä ja käyttöjärjestelmän tai tietokoneen käyttöä häiritsevillä tavoilla. Uudet virukset ovat vaikeammin huomattavissa ja ne varaavat käyttöjärjestelmälle tärkeitä tiedostoja toimintaansa varten, estäen monesti virustorjuntaohjelmiston toiminnan kokonaan ja jättäen tietokoneen täysin ilman virustorjuntaohjelmiston tai palomuurin tuomaa suojaa. (Securelist 2010.)

3.2 Toiminnan mukaiset virustyypit

Madot tarttuvat tietokoneelle tietoturva-aukkojen ja sähköpostin kautta. Matojen ja viruksien ero on tietokoneen toimintojen hidastumisessa sekä käyttäjästä riippumattomassa leviämisessä. Virus ei välttämättä häiritse tietoverkon toimintaa, vaan keskittyy enemmän tietokoneen sisäiseen tuhoamiseen, muuntelemalla ja korruptoimalla erilaisia tiedostoja sekä muuttaen niiden toimintatapaa haitallisiksi. Ne leviävät kirjoittamalla itsestään kopioita ja toisin kuin virukset, mato ei tarvitse käyttäjän toimintaa levitäkseen laajalti tietokoneen kiintolevyllä. Madot toimivat hyvin itsenäisesti ja tuhoamalla tiedostoja sekä täyttämällä tietokoneen kiintolevyä omilla kopioillaan ilman käyttäjän tietämystä. Matotartunnat vaikuttavat tietokoneeseen estämällä ja hidastamalla tietoverkon liikennettä ja tietokoneen toimintaa. Tietoverkon toiminta häiriintyy, kun mato varaa tietoverkolle tärkeää kaistaa omaan haitalliseen tarkoitukseensa. Madon varaama tietoverkon kaista saattaa aiheuttaa internetin toiminnan häiriöitä tai mahdollisesti estää sen toiminnan kokonaan. Nämä hieman ehkä yllättäenkin tapahtuvat internetverkon käytön muutokset ovat hyvin

helposti huomattavia matotartunnan merkkejä ja ne kiinnittävät etenkin internetin käyttäjien huomion hyvin nopeasti. (AntivirusWorld 2009.)

Madot leviävät helposti sähköpostien liitetiedostojen kautta. Tuntemattomien lähettäjien sähköpostiliitteiden avaaminen altistaa tietokoneen matotartunnoille, mutta tietoturva-aukot ovat vieläkin yleisempi leviämistapa. (Norton from symantec, 1.8.2006.) Windows-käyttöjärjestelmän tunnetuimmat haavoittuvaisuudet olivat Microsoft Outlook-sähköpostiohjelma, joka aukaisi uusien sähköpostien liitetiedostot kysymättä käyttäjältään lupaa avaukseen, sekä Internet Explorer -internetselaimen ActiveX-komponentti, jonka koodin tietoturva-aukkojen ansiosta mato pääsi leviämään koneeseen helposti pelkällä internetsivujen selaamisella. (Kuivanen 2005.)

Matotartunnan ehkäisee helposti olemalla tarkka sähköpostin liitetiedostojen avauksessa. Myös Windows-käyttöjärjestelmän päivittäminen suojaa tietokonetta, korjaamalla Microsoft-ohjelmistojen tietoturva-aukkoja korjataan käyttöjärjestelmän päivityksien mukana tulevilla komponenteilla. Virustorjuntaohjelmien käyttö ja ylläpito ovat myös tärkeitä apuvälineitä matotartuntojen ehkäisemiseksi ja tietoturvan säilyttämiseksi, mutta virustorjuntaohjelmilla voi olla joskus vaikeaa poistaa laajalti levinneitä matoja tartuntasijaintien vuoksi. (Kuivanen 2005.)

Uusimmat madot saastuttavat myös matkapuhelimia. Matkapuhelinselainten ja internetistä saatavien matkapuhelinohjelmistojen käytön lisäännyttyä matoja on löydetty myös yleisimmistä matkapuhelimien käyttöliittymistä. Näitä haittaohjelmia vastaan on luotu matkapuhelimissa toimivia virustorjuntaohjelmia, jotka suojaavat matkapuhelinta kaikilta mahdollisesti tarttuvilta haittaohjelmilta. Matojen toimintatapa on matkapuhelimissa samanlainen kuin tietokoneissa, mutta matkapuhelimissa ne vaikuttavat matkapuhelinverkkoon estäen ja häiriten verkon liikenteen toimintaa.

Trojan kuuluu virusten ryhmään, vaikka toimiikin hieman eri tavalla kuin perinteinen tietokonevirus, koska se ei tee itsestään kopioita. Trojanit saastuttavat tietokoneen trojan-tiedostolla varustetun ohjelman tai sovellustiedoston kautta. Kun

ohjelma tai tiedosto avataan, se tartuttaa itsensä tietokoneen kiintolevylle ja ryhtyy tekemään aukkoja tietokoneen tietoturvajärjestelmiin. Nämä trojanin aiheuttamat tietoturva-aukot vaikuttavat tietokoneen yleiseen tietoturvaan ja mahdollistavat muiden tietoturvauhkien tarttumisen tietokoneen kiintolevylle sekä internetrikollisten hyökkäykset palomuurin tai ohjelmien kautta. Trojan voi siis aukaista myös tietoliikenteen portteja, jonka avulla tietokonetta voidaan käyttää roskapostin lähettämiseen, tietomurtoihin ja palvelunestohyökkäyksiin. (Anti-trojan.org 2010.)

Trojanin sisältämät ohjelmat voivat olla päältäpäin ja ominaisuuksiltaan hyödyllisiä ja mielenkiintoisia. Osa trojan-ohjelmista on tehty hämäämään käyttäjää ja valmistettu vain haittaohjelman tartuttamiseksi käyttäjän tietokoneelle. Toiset ohjelmat ovat usein aitoja, laittomasti ladattuja ohjelmistoja, joihin on sisällytetty trojan tyyppinen virus opetukseksi laittomien ohjelmien lataamisesta. Saastunutta ohjelmaa asentaessa tai käynnistäessä aktivoituu myös haittaohjelma, pureutuen usein käyttöjärjestelmän varaamaan muistiin. Trojanin voi saada sovellusten lisäksi myös sähköpostiliitteistä.

Trojan-tartunnan voi tunnistaa tietokoneen toimintojen ja tietoverkon hidastumisena, liiallisena resurssien käyttönä, uusina kuvakkeina ja internetsivujen linkkeinä, internetsivujen ohjautumisena väärille sivuille sekä näytölle pomppaavina mainoksina. Kaikki trojanin aiheuttamat ongelmat ovat helposti tunnistettavissa, jos ymmärtää mitä trojan-haittaohjelman ominaisuudet ja seuraukset voivat saada aikaan sekä millaista tartuntatapaa se käynnistyessään voi mahdollisesti käyttää. (Anti-trojan.org 2010.)

Trojaneilla on kahdeksaa erilaista toimintatyyppiä, joista ovat yleisimpiä kauko-ohjatut trojanin versiot. *Kauko-ohjatulla trojan*illa hyökkääjä voi hallita tietokonetta etäkäyttöisesti, joilloin hänellä on mahdollisuus varastaa käyttäjän tietoja ja tiedostoja tietokoneen kiintolevyltä. Salasanoja lähettävät trojanit kopioivat vain käyttäjän erilaisiin palveluihin kirjoittamia salasanoja ja lähettävät ne eteenpäin hyökkääjän sähköpostiosoitteisiin. Ne eroavat kirjoituksen kaappaavista trojaneista siinä, että ne eivät pysty tallentamaan käyttäjän kaikkea näppäimistöllä kirjoitettua tekstiä. Kirjoituksen kaappaavat eli key logger -trojanit tekevät saamastaan tiedosta *loki-*

*tiedosto*ja, josta ohjelma tai haittaohjelman tekijä voi etsiä henkilökohtaista tietoa omaan käyttötarkoitukseensa. Trojanit voivat toimia myös tiedostoja tuhoavana ja poistavana muotona, jolloin sen toimintatapaa voidaan verrata perinteiseen tietokonevirukseen. Trojanin erilaisuutena tavalliseen tietokonevirukseen nähden on hyökkääjän mahdollisuus tuhota etäkäyttöisesti vain tiettyjä tiedostomuotoja tai aktivoida tekemänsä trojanin loogisena pommina. (Topbits.com 2010.)

Palvelunesto-, proxy/wingate- ja FTP-trojanien toimintatapana on häiritä tietoverkon toimintaa. Palvelunesto-trojan toimii samalla tavalla kuin tavalliset palvelunestohyökkäykset, mutta keskittyvät vain yhden tietokoneen tietoverkon käytön häirintään. Proxy/Wingate trojanit muuttavat tavallisen tietokoneen proxy/Wingate-serveriksi, jonka avulla hyökkääjä käyttää tietokonetta epäluotettavien internetpalveluiden isäntäkoneena. Tietokoneella voidaan trojanin avulla rekisteröidä useita internetsivuja, joiden käyttötarkoituksena on varastaa sivulla kävijöiden luottokorttitunnuksia anonyymisti. FTP-trojanit ovat näistä kolmesta trojan-muodosta yksinkertaisimpia. Niiden ainoana toimenpiteenä on avata tietokoneen palomuurista portti numero 21. Tämän portin avaamisen avulla jokainen tietoverkkoa käyttävä henkilö pääsee etäkäyttämään trojanilla tartutettua tietokonetta. Tästä trojan tyypistä on tehty myös edistynyt versio, joka antaa vain hyökkääjälle mahdollisuuden tietokoneen tiedostojen tutkimiseen oman salasanansa avulla. (TopBits.com 2010.)

Tietoturvan ylläpidolle vaarallisimpia trojaneita ovat ohjelmistoja inaktivoivat trojanin muodot, jotka pysäyttävät virustorjuntaohjelmien ja palomuurin toiminnan. Tällä trojanilla hyökkääjä saa tietokoneen kokonaan käyttöönsä ja altistaa tietokoneen muille, mahdollisesti vaarallisemmille tietoturvauhkille.

Trojan toimii varaamalla tietokoneen muistia ja suoritintehoa omaan käyttöönsä. Jokaisella tietokoneen käynnistyskerralla käynnistyy usein myös trojanin käyttämä tiedosto tai resurssi. Trojan tartuttaa itsensä käyttöjärjestelmän muistiin ja toimii usein samankaltaisilla nimillä, kuin käyttöjärjestelmälle tärkeät tiedostot ja palveut toimivat. Kyseisen ominaisuuden vuoksi trojania voi olla joskus vaikeaa huomata aktiivisten prosessien tai palveluiden listalta. Windows- käyttöjärjestelmän tehtä-

vienhallinnan kautta tietokoneen käyttäjä voi tunnistaa trojanin toiminnalle elintärkeän tiedoston sen resurssien käytön ja nimen perusteella. Jos tehtävänhallinnan resursseista löytyy trojanin käyttämä tiedosto, sen voi yrittää pysäyttää lopeta prosessi- toiminnan avulla ilman erillisiä virustorjuntaohjelmistoja. Resurssin manuaalinen pysäyttäminen voi auttaa virustorjuntaohjelmaa trojanin poistossa, koska käyttöjärjestelmän aktiivisia resursseja ei voi puhdistaa tai poistaa. Käyttöjärjestelmän käynnistyessä avautuvat trojanit voidaan pysäyttää käyttöjärjestelmän rekisteritietojen muuttamisella tai palveluiden ja ohjelmistojen erillisillä keskeyttämisellä Windows-käyttöjärjestelmän omilla työkaluilla. (Anti-trojan.org 2010.)

Resurssien keskeyttäminen ja rekisteritietojen muuttaminen mahdollistavat trojanin puhdistamisen tietokoneelta, ehkäisevät tartunnan leviämisen ja johtavat usein trojanin aiheuttamien haittavaikutuksien katoamiseen. Nämä edellämainitut keinot trojanin pysäyttämiseksi ovat etenkin tietokoneen peruskäyttäjälle usein liian vaikeita, sillä rekisteritiedostoja ei saa muuttaa tai poistaa ilman täyttä ymmärrystä mitä rekisteri-tiedostoja voi muuttaa ja tärkeiden resurssien pysäyttäminen voi pahimmassa tapauksessa kaataa käyttöjärjestelmän. Resurssien ja palveluiden pysäyttäminen sekä rekisteritiedostojen muuttaminen ei silti takaa trojanin puhdistuksen onnistumista, mutta ovat hyödyllisiä apukeinoja käyttöjärjestelmän käyttökuntoon palauttamiseksi. (Read.)

Virustorjuntaohjelma pystyy usein pysäyttämään trojanit, mutta päivittämättömät virustorjuntaohjelmat eivät voi tunnistaa uusia tietoturvauhkia. Trojan saattaa jäädä siis tarttuessaan huomaamatta ja pahimmassa tapauksessa olla aktiivisena tietokoneen muistissa useita kuukausia, ellei jopa vuosia. Päivitetty virustorjuntaohjelma on paras turva trojaneita vastaan, mutta inhimillisen tietoturvan on oltava myös kunnossa ja oman tietoverkon käytön riskit tunnistettava. Palomuuri ja sähköpostisuodattimet ovat myös hyödyllisiä trojaneiden ennaltaehkäisemiseksi, joskaan niiden tietoturva ei ole riittävä kaikille trojaneiden tyypeille. (Anti-trojan.org 2010.)

Uudet pankkitrojanit ovat vaarallisimpia trojan muotoja mitä on koskaan kohdattu. Monet uusista trojaneista varastavat pankkitietoja, erityisesti juuri käyttäjätunnuk-

sia sekä salasanoja käyttäen niitä verkkopankkia käyttävien henkilöiden tilien tyhjentämiseksi. Verkkopankit varautuvat jatkossa entistä vaikeampiin ja vaarallisimpiin pankkitrojaneihin. Toistaiseksi huijareiden ja rikollisten viemät rahasummat ovat olleet pieniä, mutta haittaohjelmat ovat kehittyneet koodiltaan nopeasti ja vakavempia haittaohjelmia sekä huijauksia on luvassa lähivuosina erittäin monia, johtuen tämän kaltaisen rikollisen toiminnan taloudellisesta hyödystä. (Lehto. 24.11.2009.)

3.3 Hoax-viestit, phishing ja spyware

Verkkopankkihuijaukset ja tietojenkalastelu eli phishing ovat viimevuosina lisääntyneet verkkopankkien käytön yleistyttyä koti- ja yritysverkoissa. Huijauksia tehdään sähköpostilla huijausviesteinä ja käyttäjätunnuksien sekä salasanojen kysymisellä oikeaksi naamioiduilla verkkopankkien kirjautumissivuilla. Tunnuksia ja salasanoja antaessa pitääkin olla erityisen varovainen mitä on tekemässä sekä selvittää tarkkaan verkkopankin turvallisuus ja sivuston alkuperä. Huijarit tekevät sivustoja jotka ovat täysin samannäköisiä kuin oikeat verkkopankkien internetsivut. Huijareiden verkkopankkisivuston sisäänkirjautuminen kopioi käyttäjän tunnuksen ja salasanan, eikä käyttäjä lopulta edes pääse kirjautumaan verkkopankin palveluun. Huijareiden tekemillä verkkopankkisivustoilla ei ole kuitenkaan aitoa *varmenne*tta, jonka avulla jokainen käyttäjä voi tunnistaa mahdollisen huijauksen ennen tunnuksen ja salasanan antamista rikollisten käsiin. Tämän varmenteen voi aina tarkistaa internetselaimen alapalkissa sijaitsevasta varmennekuvakkeesta. Verkkopankkeja käyttävien tilitietoja urkitaan myös erilaisilla tekosyillä, kuten olemattomilla huoltokatkoilla ja huoltokatkojen ajaksi tehdyllä erilaisella kirjautumislaatikolla. (Lehto. 24.11.2009.)

Tulevaisuudessa verkkopankkeja käyttävät henkilöt tulevat saamaan apua laajakaistaliittymien operaattoreilta, jotka tunnistavat verkkopankkihuijaukset ilmoittamalla mahdollisen tietoturvauhkan olemassaolosta. Tämä suojaa kokemattomia ja kokeneita internetin käyttäjiä, koska operaattori reagoi tietoturvauhkaan ja toimii tarvittavalla tavalla haittaohjelmien ja hyökkäyksien estämiseksi. Operaattoreiden

avun mahdollistaa Lex Nokia -tietosuojalaki, joka sallii verkkoliikenteen suodattamisen väliaikaisesti juuri phishing- ja urkintaliikenteen estämiseksi. Ennen Lex Nokian toimeenpanoa on voitu suodattaa vain viruksia ja sähköpostia, mutta uusi laki täydentää verkkopankkien tietoturvaa tietoliikenteen suodattamisella. (Lehto. 24.11.2009.)

Muita verkkopankkien tietoturvaa nostavia seikkoja ovat myös juuri käyttöönotetut tekstiviestivahvistukset suurten summien omaavien laskujen maksussa. Tekstiviestivahvistusta varten verkkopankkiin on tallennettava oma matkapuhelinnumero. Vahvistus on maksuton, yksinkertainen ja turvallinen tapa ottaa mukaan uusi turvavarmistus verkkopankkien käyttäjille. Pankit tiukentavat pian myös rahaliikenteen valvontaa mahdollisten rikollisten tilitapahtumien tunnistamiseksi, jotta verkkopankkien käyttö pysyisi turvallisena ja vaivattomana. (Lehto. 15.2.2010.)

Spyware on vakoiluohjelma, joka kerää tietoja tietokoneen ja tietoverkon käyttäjästä. Vakoiluohjelma tutkii käyttäjän verkkokäyttäytymistä ja välittää saamaansa tietoa eteenpäin internetiin. Kerättävä tieto voi sisältää käyttäjätunnuksia, salasanoja, käytettyjen tiedostojen nimiä ja kaikkea mahdollista tietoa, minkä avulla vakoiluohjelma voi saada mainosohjelmia ja -postia lähetettyä kohdistetusti tietyille asiasta kiinnostuneille henkilöille. Vakoiluohjelma voi myös nauhoittaa ja seurata internetissä käytäviä puheluita, keskusteluja sekä erillisiä keskusteluohjelmia. (Microsoft .)

Suurin osa vakoiluohjelmista asentuu tietokoneen kiintolevylle itsestään ilman erillistä asennusikkunaa tai kehotetta ja sen olemassaolo huomataan mainoksien ponnahdusikkunoina sekä internetselaimen aloitussivun yllättävällä vaihtumisella. Vakoiluohjelmat leviävät sähköpostin sekä erilaisten ilmaisten ohjelmistojen ja internetsivujen kautta.

Vakoiluohjelmien komponenttejä sisällytetään myös haittaohjelmien lisäksi ilmaisiin ja maksullisiin hyöty- ja apuohjelmiin. Virustorjuntaohjelmistot eivät tunnista vakoiluohjelmien olemassaoloa, sillä ne tulevat usein sellaisten ohjelmien mukana, minkä asentaminen tarvitsee käyttäjän suostumuksen asentaessa. Tämä

asentamiseen suostuminen sisältää Terms of Agreement -sopimustekstin, jossa saatetaan ilmoittaa vakoilukomponentin olemassaolosta. Tietokoneen käyttäjät harvoin lukevat tätä tekstiä ja asentavat ohjelmat nopeasti. Tällöin vakoilukomponentti asentuu käyttäjän luvalla ohjelman kannalta laillisesti. Laillisesti asennettavaksi suunnitellut vakoiluohjelmat ovat tietoturvaohjelmille usein tunnistamattomissa. Tässä tapauksessa vakoiluohjelman poistoon tarvitaan muita, tehokkaampia ohjelmia tai asennetun ohjelman poistoa. (Kautiala. 2004. 171 – 174.)

Palvelunestohyökkäys käyttää tietokoneen resursseja ja internetyhteyden kapasiteettia tietoverkon hidastamiseksi. Hyökkäyksen aikana tietoverkon käyttö häiriintyy ja internetiä voi olla mahdotonta käyttää. Palvelunestohyökkäyksen tarkoituksena ei ole tunkeutua käyttöliittymän järjestelmään ja varastaa sieltä tietoja, sillä sen tavoitteena on häiritä tietokoneen käyttöliittymän ja tietoverkon toimintaa.

Julkisissa tietoverkoissa palvelunestohyökkäykset kuormittavat internetsivuja ja sähköpostipalvelimia, jotta asiakkaat eivät voi käyttää niitä tai saada sähköpostiaan perille hyökkäyksen kohteena olevaan osoitteeseen. Toukokuussa 2007 Eniron, Ylen ja Suomi24-internetsivut joutuivat palvelunestohyökkäyksien kohteeksi. Internetsivujen käyttö oli tuolloin mahdotonta tahallisen häiriköinnin myötä. Palvelunestohyökkäyksien hyökkääjien tarkoituksena oli vain häiriköidä sivujen toimintaa ja teosta ei ollut heille taloudellista hyötyä. (Cert-fi 15.5.2007. 22.5.2007.)

Erilaisten palvelunestohyökkäysmuotojen tunteminen ei ole kovinkaan tarpeellista, sillä tietokoneen peruskäyttäjä ei voi tehdä palvelunestohyökkäykselle yleensä yhtään mitään. Palvelunestohyökkäyksen uhriksi joutuessaan henkilön täytyy ottaa yhteyttä internetpalveluntarjoajaan, joka auttaa ja antaa tietoa mitä on hyökkäyksen aikana on tapahtunut ja mitä tietokoneelle tulee tehdä hyökkäyksen jälkeen. Edistyneemmät käyttäjät voivat vaihtaa itse hyökkäyksen aikana vaarantuneen IP-osoitteensa ja säätää palomuurin sekä tietokoneen asetuksia uusien hyökkäysten torjumiseksi. Usein hyökkäyksen jälkeen joutuu vaihtaamaan tietokoneen verkko-

kortin tai ainakin verkkokortin MAC-tunnuksen sekä tietokoneella käytettävän osoitteen jäljittämisen estämiseksi. (Jansson 2010.)

Palvelunestohyökkäyksiä on neljää erilaista muotoa, joista *tulvahyökkäyks*et (SYN Flood) ovat palvelunestohyökkäyksien yleisin ja yksinkertaisin muoto. Ne eivät hyökkää itse käyttäjän tietoverkkoihin, vaan keskittyvät julkisien internetsivustojen kuormittamiseen ja sähköpostipalvelimien tilan täyttämiseen roskapostilla. Tämä vaikuttaa internetin käyttäjään vain hyökkäyksien kohteena olevilla internetsivustoilla vieraillessa, sillä sivua ei voi hyökkäyksen alaisena käyttää ollenkaan. Tällaisissa hyökkäyksessä väärinkäytetään yhteydellisen TCP-protokollan yhteydenmuodostuspaketteja (SYN), joihin sivustojen kohdepalvelin vastaa. Hyökkäyksissä jätetään kohdepalvelimen vastauksen odottaminen tahallaan kesken, jolloin palvelin jää odottamaan yhteyden muodostumista varaten turhaan resursseja hyökkäyksen kohteena olevilta palvelimilta ja palomuureilta. (Jansson 2010.)

Tietokoneen käyttäjiin vaikuttavampia hyökkäyksiä ovat tietoliikenteen ohjaustietojen häiritseminen, vääränlaiset lähetteet ja istuntojen määrien kasvattaminen palomuurin tukkeutumiseksi. Ohjaustietojen häiritseminen vaikuttaa reitittimen asetuksiin muuttamalla lähetettävien datapakettien osoiteet vääriksi. Tämä aiheuttaa internetin käyttäjälle vaaratilanteita, sillä hyökkäys uudelleenohjaa suosituilla internetsivuilla kävijän rikollisten varaamalle palvelimelle. Vääränlaiset lähetteet vaikeuttavat Windows-käyttöjärjestelmän käyttöä ja kaatavat käyttöjärjestelmän palvelinohjelman. Käyttöjärjestelmä kaatuu hyökkäyksen tapahtuessa siniseen ruutuun ja tietokone on käynnistettävä uudelleen hyökkäyksestä selviytyäkseen. Palvelunestohyökkäys jossa nostetaan käytössä olevien istuntojen määrää, tukkii palomuurin toiminnan avaamalla uusia tietoliikenneyhteyksiä. (Jansson 2010.)

Hajautetut palvelunestohyökkäykset tehdään botnet- haittaohjelman avulla. Sillä pystytään ottamaan etähallinnalla haltuun tietokoneita ja yhdistämään ne verkostoksi, jolla voidaan osallistua palvelunestohyökkäyksiin. Tietokonetta voidaan käyttää hyökkäykseen käyttäjän tietämättä, sillä tietokoneen virustorjuntaohjelmistot eivät välttämättä tunnista palvelunestohyökkäyksissä käytettäviä haittaohjelmia, verkkomatoja tai haitallista vertaisverkkosovellusta. (Cert-fi 31.5.2007.)

3.4 Inhimilliset uhkatekijät

Osa internetin käyttäjistä kotona ja yrityksissä syyllistyy tietoturvan laiminlyöntiin tietoisesti tai tiedostamattomasti jopa päivittäin. Tietoturvan laiminlyönti tarkoittaa henkilön suhtautumista tietoturvaa koskeviin uhkiin. Välinpitämättömyys ja tietämättömyys ovat inhimillisten tietoturvauhkien pääsyinä. Välinpitämättömyys omaa tietoturvaa kohtaan on yksi tietokoneen käyttäjien suurimmista inhimillisistä virheistä. Se vaikuttaa tietokoneen haittaohjelmien ennaltaehkäisyyn, puhdistamiseen ja tietoturvan ylläpitoon negatiivisesti, aiheuttaen useita tietoturvauhkia käyttäjän tietokoneelle, mahdollisesti levittäen haittaohjelmia eteenpäin toisille tietoverkkoa käyttäville henkilöille.

Suurimpia inhimillisiä uhkatekijöitä ovat virustorjuntaohjelman puuttuminen tietoisesti ja tiedostamatta sekä tietoinen tietoturvan vaarantaminen omalla välinpitämättömällä käytöksellään. Monilta tietokoneilta puuttuu virustorjuntaohjelma kokonaan pelkästään sen vuoksi, että käyttäjä ei ole tietoinen sen tuomasta turvasta ja mahdollisesta tarpeesta. Tietokoneen käytön aloittavat käyttäjät eivät välttämättä osaa asentaa tai valita omalle tietokoneelleen sopivaa virustorjuntaohjelmistoa. Tietoisesti käyttöjärjestelmästä poistettu tai pois jätetty virustorjuntaohjelma on tietoturvauhkien leviämiselle erittäin altis ympäristö. Virustorjuntaohjelman puuttuminen altistaa tietokoneen vaarallisille tietoturvauhkille ja henkilökohtaisen tiedon varastamiselle. Ilman virustorjuntaohjelmaa käyttäjä ei ole tietoinen tietokoneeseen tarttuneista viruksista ja haitallisista tiedostoista, eikä osaa reagoida oikein haittaohjelmien mahdollisesti tuomiin ongelmiin ja siihen miten uhka puhdistetaan tietokoneelta.

Virustorjuntaohjelman asennus on yleensä helppoa ja ilmaisia ohjelmistoja löytyy useita jopa suomenkielisinä. Rahan ja kiintolevytilan puute ei ole mikään syy jättää virustorjuntaohjelmistoa pois tietokoneelta. Jokaiselle tietokoneelle ja käyttäjälle löytyy sopiva virustorjuntaohjelmisto, oli se sitten maksullinen tai maksuton ja suomen- tai englanninkielinen. Ohjelmistoja täytyy kokeilla itse ja lukea myös muiden ohjelmistoa käyttäneiden mielipiteitä ohjelman toiminnasta ja käytöstä, sekä tutkia virustorjuntaohjelman järjestelmävaatimuksia. Jos käyttäjä ei osaa valita itselleen

virustorjuntaohjelmistoa, voi hän ostaa virustorjunnan internetoperaattorilta ja saada operaattorilta apua ohjelman asentamiseen ja käyttöön. Virustorjuntaohjelman rinnalle on suotavaa asentaa vakoiluohjelmien ja muiden haittaohjelmien poistoa ja torjuntaa varten toinen haittaohjelmia torjuva tai poistava ohjelma, mutta ei toista virustorjuntaohjelmistoa, sillä se saattaa vaikuttaa tietokoneella jo ennaltaan olevan virustorjuntaohjelmiston toimintaa. Virustorjuntaohjelmiston ylläpito on hyvin helppoa. Kun ohjelmiston käyttöaika eli lisenssi päättyy, täytyy käyttäjän hankkia ohjelmalle lisää aikaa tai vaihtaa toiseen ohjelmaan. Virustorjuntaohjelmistot lataavat itse päivityksensä, ellei tietokoneella ole haittaohjelmaa, joka estää virustorjuntaohjelmiston yhteyttä ohjelmiston verkkopalvelimeen.

Virustorjuntaohjelmat ovat aina hyödyllisiä ja välttämättömiä PC:n tietoturvan säilymiseksi. Palomuurin käyttäminen ja päälläpito on myös erittäin tärkeää, eikä palomuurin portteja saisi avata ohjelmistojen toimintaa varten. Edistyneet tietokoneiden käyttäjät säätelevät virustorjuntaohjelmia ja palomuuria käyttötarkoitustaan vastaaviksi, mutta valitettavan usein virustorjuntaohjelmat ja palomuuri otetaan kokonaan pois käytöstä. Virustorjuntaohjelmiston tuoma suojaus on tärkeä ase tietoturvauhkien leviämistä vastaan ja vaikka tietokoneella olisikin virustorjuntaohjelmisto, sen toiminnan ylläpitoa, reaaliaikaista tarkistusta ja ennaltamäärättyjä virustarkastuksia laiminlyödään helposti ajattelematta mahdollisia seurauksia. Ohjelmien päivitysten laiminlyönti vaikuttaa virustorjuntaohjelman toimintaan ja tietoturvan tasoon negatiivisesti. Virustorjuntaohjelmat tarvitsevat uusia päivityksiä, jotta ne pystyvät huomaamaan uusien tietoturvauhkien tarttumisen sekä tietävät miten tiedoston voidaan puhdistaa. Myös virustarkastusten peruuttaminen ja pysäyttäminen heikentävät tietoturvauhkien löytymistä ja hidastavat niiden puhdistamista. Kyseisten toimintojen laiminlyönti saataa aiheuttaa vaarallisten uhkien tartunnan tietokoneelle ja tuhota kiintolevyn tiedostoja ilman käyttäjän tietoa mahdollisesta tartunnasta.

Reaaliaikainen virustarkastus huomaa usein tarttuneet tiedostot välittömästi tartunnan tapahduttua, mutta myös tämä tärkeä virustorjuntaohjelmiston ominaisuus on helposti laiminlyönnin kohteena. Reaaliaikaiset ja automaattiset virustarkastukset heikentävät varsinkin vanhojen tietokoneiden toimintakykyä kuluttamalla tie-

tokoneen resursseja sekä muistia. Jos tietokone käyttää reaaliaikaista tarkistusta, kannattaa miettiä onko tietokone tarpeeksi tehokas virustorjuntaohjelmiston käytölle. Automaattisia virustarkistuksia voidaan asettaa tapahtuvaksi sopivina ajanjaksoina, milloin tietokone voidaan pitää päällä ja sitä ei käytetä aktiiviseksi. Virustorjuntaohjelmistot ovat pääasiassa hyvin joustavia näiden virustarkistusmuotojen kanssa. Tarkistusten peruminen tai pois päältä asettaminen on yleensä käyttäjän omaa laiskuutta. Mitä vanhempi tietokone käyttäjällä on, sitä useammin virustarkistuksia laiminlyödään. Uusilla tietokoneilla tarkistukset ovat todella kevyitä ja niiden tapahtumista tuskin edes huomataan. Jos virustorjuntaohjelmisto on kuitenkin liian raskas tietokoneen järjestelmälle, kannattaa etsiä uusi ja mahdollisimman kevyt ohjelmisto vanhan tilalle, tai jos tietokone on jo hyvin vanha, kannattaa miettiä olisiko aika vaihtaa uuteen tietokoneeseen oman tietoturvan tähden.

Palomuurin puuttuminen tai sen asettaminen pois päältä on myös vaarallista tietoturvan kannalta. Palomuuri laitetaan usein pois päältä, koska se vaikuttaa tietokoneen tietoliikenteen kulkuun haitallisesti. Edistyneet tietokoneen käyttäjät laittavat palomuurin pois päältä tietoisesti, koska se vaikuttaa internetiä käyttävien ohjelmistojen toimintaan hidastavasti tai estää ohjelmille tärkeiden verkkoyhteyksien muodostamisen. Myös palomuurin porttien avaaminen tiettyä ohjelmaa varten vaikuttaa tietoturvan tasoon heikentävästi ja sitä tulisi välttää, mutta portteja avataan valitettavan usein. Windows-käyttöjärjestelmän oma palomuuri jää usein peruskäyttäjien tietokoneilla päälle, koska sen olemassaolosta, toiminnasta ja merkityksestä tietoturvan suojaamiseksi ei juurikaan tunneta.

Monet edistyneemmät tietoverkkojen käyttäjät lataavat tietokoneelleen P2P-ohjelmia, joilla ladataan ja jaetaan erilaisia tiedostoja laittomasti. Tätä ohjelmaa käyttämällä he altistavat tietokoneensa haavoittuvaiseksi erilaisille tietoturvauhkille, erityisesti trojaneille. *P2P-ohjelma*lla ladattavat tiedostot, kuten ohjelmistot ja pelit voivat sisältää sovellustiedoston (.exe), jota aktivoittaessa asentuu tietokoneelle myös haittaohjelmia ja viruksia. Jos P2P-ohjelmia haluaa välttämättä käyttää laittomaan lataukseen, ohjelmalla ladatut tiedostot tulisi tarkastaa ennen asennusta tai sovelluksen käynnistämistä. P2P-ohjelmien käyttö on tietoinen tietoturvan laiminlyönti ja sen käyttäminen ei ole välttämätöntä tietoverkkoa käyttäville henki-

löille. Onneksi kuitenkaan aloittelijat tai tietokoneen peruskäyttäjät eivät osaa käyttää näitä monimutkaisia P2P-ohjelmia ja pysyvät turvassa näiden ohjelmistojen kautta leviäviltä haittaohjelmilta.

Jokainen tietokoneelle ladattu tiedosto olisi hyvä tarkistaa joko internetissä sijaitsevilla online skannereilla tai tietokoneelle asennetulla virustorjuntaohjelmistolla ennen tiedoston asennusta tai avaamista, vaikka tiedosto olisikin ladattu luotettavasta lähteestä. Minuutin kestävä virustarkastus on helppo ja nopea vaihtoehto mahdollisten haittaohjelmien leviämisen ja tartunnan seurausten näkökulmasta. Pieni vaiva tiedostojen tarkistuksessa on arvokas asia tietoturvan säilyttämiseksi. Valitettavasti useita tarttuneita haittaohjelmia ei huomata, ennen kuin pahin on jo ennättänyt tapahtua. Pahimmassa tapauksessa haittaohjelmat varastavat luottokortti- ja pankkitietoja, vieden verkkopankkien käyttäjien pankkitileiltä rahaa. Virukset aiheuttavat myös tuhoa Windows-käyttöjärjestelmälle niin, että tietokoneen käyttöjärjestelmä on asennettava uudelleen ja kiintolevy on alustettava kokonaan. Torjunta-keinot ja haittaohjelmia torjuvien ohjelmien ylläpito on paljon yksinkertaisempaa ja helpompaa, kuin tietokoneen ja itsensä altistamisen tietoturvauhkille, jotka pahimmassa tapauksessa voivat tuhota kokonaisen yrityksen tai yksittäisen tietoverkkoa käyttävän elämän. (Jansson 2010.)

Eräs tietoturvauhkien suurimmista tartuntasyistä on sähköpostiliitteiden avaus ilman erityistä huomiota siihen, mitä liitetiedosto sisältää tai mistä se on lähetetty. Monet laajalti levinneet haittaohjelmat ovat saaneet alkunsa muutamana sähköpostin kautta lähetettynä sähköpostiliitteenä. Sähköpostin käyttäjät kiinnittävät valitettavan vähän huomiota sähköpostiliitteiden turvallisuuteen, sisältöön ja alkuperään. Sähköpostipalvelut ja virustorjuntaohjelmistot ovat kiinnittäneet tähän seikkaan huomiota ja tarjoavat sähköpostin käyttäjälle suojaa liitteiden mukana tulevia tietoturvauhkia vastaan. Koska sähköpostiliitteiden avulla laajalti levinneitä viruksia on hyvin monta, myös media huomauttaa internetin käyttäjiä liikkeellä olevista vaarallisista sähköposteista. Median tuoma huomio asiaa kohtaan on tuonut tietoa sähköpostin käyttäjille hyvin paljon, mutta monet laiminlyövät ja aliarvioivat uhkien todellisuutta ennenkuin on liian myöhäistä ja sähköposti on jo avattu.

Aiemmat sähköpostiohjelmat, kuten Microsoft Outlook, oli yksi suuremmista tiedostamattomista inhimillisistä tietoturvauhkista. Kyseinen sähköpostiohjelma avasi tulleiden sähköpostien liitteet ilman käyttäjän hyväksyntää ja liitteen mukana tullut haittaohjelma levisi tietokoneelle yllätyksellisesti. Tämän kaltaiset ohjelmistot ovat suurin syy, miksi sähköpostiliitteiden mukana leviävät tietoturvauhkat yleistyivät ja jatkavat helppoa leviämistään maailmanlaajuisessa tietoverkossa. Sähköpostipalveluiden ja virustorjuntaohjelmistojen huomautukset vaarallisista liitteistä, vaarallisten liitteiden avauksen esto, automaattiset liitteiden virustarkastukset ja liitteiden avaus erillisellä kysymyksellä, ovat tuoneet inhimilliselle tietoturvalle pientä helpotusta sähköpostin tietoturvauhka tekijöiden tietoturva ratkaisuilla. Monet tietokoneen peruskäyttäjät omaavat sähköpostitilejä monissa eri sähköpostipalveluissa ja ovat jatkuvasti monien tietoturvauhkien uhreina ja haittaohjelmien lähetyksen kohteina.

Windows-käyttöjärjestelmän päivitysten laiminlyönti on hyvin yleinen inhimillinen tietoturvanuhkatekijä ja altistaa käyttöjärjestelmän virustartunnoille sekä haittaohjelmien leviämiselle. Päivittäminen on uusimmissa virustorjuntaohjelmissa ja käyttöliittymissä automaattista, eikä vaadi käyttäjältään manuaalista päivityspalvelimeen yhdistämistä. Automaattisen päivityksen saa myös asetettua pois päältä, jolloin käyttäjä laiminlyö tietoturvaa tietoisesti. Käyttöjärjestelmän kaikkia löydettyjä päivityksiä ei tarvitse asentaa, mutta tietoturvapäivitysten asentaminen on joissain tapauksissa välttämätöntä tietoturva-aukkojen korjaamiseksi. Joitain päivityksiä varten tarvitaan tietokoneen uudelleen käynnistystä, eikä muuta tarvitse tehdä, mutta osa käyttöjärjestelmän päivityksistä voivat aiheuttaa tietokoneelle monia toiminnallisia ongelmia, esimerkiksi tietokoneen käynnistyksen vaikeutumista ja hidastusta. Näiden edellä mainittujen syiden vuoksi, päivityksiä laiminlyödään ja jätetään asentamatta. Windows-käyttöjärjestelmän tietoturva-aukot ovat olleet jo vuosia suuria tietoturvan uhkatekijöitä ja tietoturvapäivitysten lataaminen on välttämätöntä tietoturvauhkien ehkäisyssä, mikäli Windowsia halutaan käyttää.

Inhimillisiä tietoturvauhkia voidaan torjua parhaiten tietoverkon käyttäjän asenteen muutoksella ja järjen käytöllä. Pienet muutokset omassa käytöksessä auttavat huomattavasti oman tietoturvan säilyttämisessä ja parantamisessa. *Netiket*in nou-

dattaminen tietoverkkoa käyttäessä on hyvä opetella ulkoa tai tulostaa vaikka tietokoneen viereiselle seinälle. Inhimillinen tietoturva ei koske vain tietokoneen peruskäyttäjiä, sillä osa tietoturvaa laiminlyövistä henkilöistä ovat käyttäneet tietoverkkoja jo monia vuosia. Peruskäyttäjissä on myös sellaisia henkilöitä, jotka ovat ymmärtäneet tietoverkon käytön vastuun ja rajoitukset sekä tietoturvauhkien ennaltaehkäisyn merkityksen tietoturvan säilyttämiseksi.

Mitä vakavemmat ja vaikeat haittaohjelman tartunnan seuraukset ovat, sitä enemmän ne auttavat käyttäjää oppimaan ja ymmärtämään oman tietoturvan ylläpidon tärkeyden. Kun tietokoneen käyttäjä ensimmäistä kertaa joutuu virustartunnan uhriksi, hän kiinnittää tietoturvaan jatkossa enemmän huomiota. Tietoturvauhkan vakavuudesta riippuen käyttäjä voi joutua korjaamaan tietoturvaohjelmistoilla tietokoneen saastuneita tiedostoja. Tässä vaiheessa käyttäjä joutuu asentamaan tietokoneelleen virustorjuntaohjelmiston tai haittaohjelmien poisto-ohjelman, joka korjaa laiminlyönnin aiheuttamat seuraukset, jollei virustorjuntaohjelmistoa ole asennettu tietokoneelle ollenkaan. Jos haittaohjelma ei ole vaikuttanut tietokoneella sijaitsevan virustorjuntaohjelman toimintaan, kannattaa ohjelma päivittää ennen virustarkistuksen aloittamista.

Virusten ja haittaohjelmien poistaminen on joskus hyvinkin työlästä ja voi kestää useita kymmeniä tunteja riippuen tietoturvauhkan vakavuudesta ja käyttäjän omista tietokonetaidoista. Uhkatekijän poistamisesta koituva työ antaa käyttäjälle usein hyvän syyn edistää oman tietokoneensa tietoturvaa ja kertoa myös muille tietokoneiden käyttäjille uhkien todellisuudesta. Viimeistään tietoturvan laiminlyöjän pankkitilin tyhjetessä käyttäjä reagoi niin vahvasti, että nostaa tietoturvansa tasoa ja lopettaa itsensä ja muiden käyttäjien altistamisen vakaville tietoturvauhkille. Osa tiedostetuista inhimillisistä tietoturvan laiminlyönnistä on tehty tarkoituksella, eikä käyttäjällä ole välttämättä halua oppia virheistään ollenkaan, jos se haittaa liikaa hänen tietokoneensa joka päiväistä käyttöä. Tiedostetuista tietoturvan uhkatekijöistä vakavimpia ovat piratismin edistäminen käyttämällä laittomasti ladattuja ohjelmistoja sekä ladattujen ohjelmistojen jakaminen P2P-ohjelmilla. Laittomat ohjelmat ja käyttöliittymät altistavat tietokoneita tietoturvauhkille tärkeiden päivityksien puutteen ja tiedostojen mukana tulevien haittaohjelmien vuoksi.

4 TIETOTURVAUHKIEN TORJUNTA JA ENNALTAEHKÄISY

Ensimmäinen virustorjuntaohjelma tehtiin vuonna 1987. (Antivirus software pro 2009.) Ennen internetin käytön yleistymistä virukset levisivät levykkeen ja muiden tiedon-siirtovälineiden kautta tietokoneelta toiselle. Levykkeitä varten käytettiin viruksen tunnistusohjelmaa, jota päivitettiin todella harvoin, johtuen viruksien vähäisyydestä ja tartunnoiden harvinaisuudesta. Tietoturvauhkien ennaltaehkäisyä varten on tehty monia teknisiä ratkaisuja, kuten virustorjuntaohjelmat sekä palomuurit. Nämä eivät kuitenkaan estä inhimillisistä syistä tarttuneita tietoturvauhkia, mitkä ovatkin suurin syy tämän hetkiselle tietoturvan turvattomalle tilalle.

Yksi suurimmista tietoturvauhkien leviämiskohteista on sähköposti, jota käyttäessä tulisi olla erittäin varovainen ja kriittinen tiedon luotettavuudesta. Sähköpostissa ei saa antaa henkilökohtaisia tietoja tuntemattomille tai tutuille. Liitetiedostoiden kanssa täytyy tutkia tarkkaan, mistä lähteestä tiedosto on lähetetty ja mitä se sisältää. Liitetiedoston pitää tulla tunnetusta lähteestä ja se kannattaa tarkastaa virustorjuntaohjelmalla ennen tiedoston avaamista, vaikka lähde olisikin tunnettu. Sähköpostin mukana tulevat tietoturvauhkat löytyvät usein virustorjuntaohjelmalla, mutta paras nyrkkisääntö sähköpostin kautta tarttuvien tietoturvauhkien ehkäisemiseksi olisi välttää kaikkien liitetiedostoiden avaamista, mutta käytännössä tämä on mahdotonta.

Sähköpostien liitetiedostoista doc- ja pdf-päätteiset tiedostot ovat vaarallisimpia sähköpostia käyttävälle henkilölle. Pdf-tiedostoihin tehdyt virukset ovat yleistyneet räjähdysmäisesti pdf-formaatin yleistyessä, ja niiden välttäminen on tärkeää kunnes ohjelmiston suurimmat haavoittuvaisuudet ovat korjattu. Adobe Acrobat -ohjelman ja pdf-formaatin tietoturva-aukot ovat saaneet internetrikolliset hyvin aktiivisiksi ja käyttämään hyväksi Adoben tietoturva-aukkoja uusia haittaohjelmia tehdessään. (Kotilainen. 17.2.2010.)

Yleisesti internetin käytössä täytyy olla varovainen ja käytettävä harkintakykyä millaisilla internetsivuilla vierailee ja mitä internetissä tekee. Omien tietojen antami-

nen tuntemattomille henkilöille ja sähköpostissa niitä kysyville on erityisen kiellettyä. Netiketti antaa jokaiselle internetin käyttäjälle perussäännöt, joita jokaisen tietoverkkoa käyttävän henkilön tulisi noudattaa päivittäisessä käytössä.

Tahallisesti tehtyjä uhkatekijöitä varten tarvitaan myös käyttäjästä riippumatonta tekniikkaa, joka ennaltaehkäisee tietoturvauhkia reaaliaikaisesti tietoverkon monilla eri osa-alueilla. Tätä varten on tehty virustorjuntaohjelmistoja, palomuuriratkaisuja ja muita tietokonetta ja tietoverkkoa suojaavia ohjelmia. Jokaisessa tietokoneessa tulisi olla virustorjuntaohjelmisto tiedostojen ja tietojen suojaamiseksi. Ilman virustorjuntaohjelmistoa tietokone on alttiina vaarallisille ja vaarattomille haittaohjelmille, viruksille, madoille, tietoja varastaville trojaneille sekä keyloggereille. Jos tietokoneessa ei ole virustorjuntaohjelmistoa, sellaisen voi ladata internetistä ilmaiseksi tai ostaa käyttöönsä sellainen joko erikseen tai internetoperaattorin palveluna. Virustorjuntaohjelmisto ei ole pettämätön suoja tietoturvauhkia vastaan, mutta se on yksinkertainen ja helppo, käyttäjästä riippumaton, tekninen ratkaisu tietoturvauhkien ennaltaehkäisemiseksi.

Virustartunnan voi yleensä puhdistaa virusohjelmalla. On myös viruksia, joiden puhdistamiseen tarvitaan niitä varten erikseen suunniteltuja ohjelmia. Virus voi estää virustorjuntaohjelmien toiminnan ja tässä tapauksessa tartunnan uhri joutuu usein etsimään internetistä erilaisia puhdistusohjelmia, joihin virus ei voi vaikuttaa ja joilla sen voi puhdistaa turvallisesti vaurioittamatta käyttöjärjestelmää. Virustartunta voi häiritä tietokoneen käyttöjärjestelmän käyttöä estäen sen toiminnan kokonaan. Tällöin ainoa puhdistustapa on alustaa tietokoneen kiintolevy, joka tyhjentää kaikki tietokoneen kiintolevyllä sijaitsevat tiedostot, mukaanlukien ne tiedostot joihin virus on voinut tarttua tai on tarttunut.

4.1 Virustorjuntaohjelman toiminta

Kun uusi virus havaitaan, virustorjuntaohjelmien ylläpitäjät keräävät virusten tunnistustiedot virustietokantaan. Viruksen tunnistaa sen omasta ainutlaatuisesta allekirjoituksesta, joka koostuu tietokoneen lukemista merkkisarjoista. Kun virus tart-

tuu tietokoneelle, virustorjuntaohjelma asettaa saastuneen tiedoston automaattisesti karanteeniin ja esittää hälytysikkunan. Karanteenissa virus ei pysty kopioimaan itseään ja leviämään tietokoneen sisällä tai tietoverkossa. Karanteenin jälkeen ohjelma yrittää poistaa viruskoodin ja korjata vahingoittuneet tiedostot. Karanteenissa olevat tiedostot voi poistaa ilman erityisiä seuraamuksia käyttöjärjestelmän toiminnalle. (Symantec 2010.)

Uudet monimutkaisemmat virukset aiheuttavat suurimmat haasteet virustorjuntaohjelmistojen käytölle ja uusien viruksien löytäminen sekä poistaminen on yhä vaikeampaa. Tällöin käyttäjän on pakko reagoida uhkatilanteeseen säilyttääkseen tietoturvansa ja estääkseen viruksien leviämisen. Useat virukset tarttuvat Windows-käyttöjärjestelmän toiminnalle tärkeisiin tiedostoihin, jolloin virusohjelma ei voi suorittaa tarvittavaa puhdistustoimenpidettä. Tälläiset tapaukset johtavat usein tietokoneen kiintolevyn alustukseen ja käyttöjärjestelmän uudelleen asennukseen.

Virustorjuntaohjelmilla on erilaisia virusten etsintämetodeja. Yleisin metodi on käyttää tiettyä virustietopankkia, jonka avulla ohjelma löytää saastuneet tiedostot ja virukset. Tämä metodi ei ole täydellinen uusien tuntemattomien viruksien löytämisessä, koska viruksen tietoja ei löydy virustietokannasta. Uudet kehittyneemmät virukset muuttavat ohjelmakoodiaan jatkuvasti tai piilottautuvat näkyvistä. Tällöin virustietokantaa käyttävä metodi on huono vaihtoehto virusohjelman toiminnan ja tehokkuuden kannalta. Virusohjelmistot joutuvat päivittämään virustietokantaa hyvin useasti uusien viruksien tunnistamisen jälkeen. Tietokoneiden käyttäjät voivat antaa tietoja uusista viruksista ohjelmiston kehittäjälle tutkittavaksi, jotta uudet virukset saataisiin myös muiden tietoverkkoa käyttävien henkilöiden tietoisuuteen. (de la Cuadra 2003.)

Uudet virustorjuntaohjelmistot käyttävät heurestista analyysiä haittaohjelmien tunnistamiseen. Monet virukset alkavat yhdellä tartunnalla ja mutaation tai koodin muutoksilla, niiden määrä voi kasvaa jopa kymmeniin erilaisiin virusmuunnoksiin. Virustorjuntaohjelmistojen päivityksissä ohjelma saa itselleen virustietokantaan muunnoksia jo aikaisemmin löydetyistä viruksista. Koodimuunnoksen kohteena olevat virukset voivat toimia alkuperäisestä viruksesta poikkeavalla tavoin, vaikka

viruksen nimi olisikin hyvin samankaltainen. Muunnelluilla viruksilla on kuitenkin sama geneettinen merkkinsä, joka vaikuttaa virusmuunnosten löytymiseen erilaisilla virustorjuntaohjelmistoilla. Virustorjuntaohjelmistojen valmistajat käyttävät löytämistään haittaohjelmista erilaisia nimiä, vaikka virus olisikin sama. Jos viruksesta etsitään tietoa internetistä, kannattaa siis muistaa, että viruksella voi olla monta eri nimeä.

Virustorjuntaohjelmistot helpottavat tietokoneen käyttäjän vastuuta tietoturvauhkista. Ohjelma suojaa tietokonetta ilman erityisiä toimenpiteitä ja poistaa tartunnat niiden tarttuessa, eikä käyttäjällä tarvitse olla tietoa ja kokemusta viruksista tai virustorjuntaohjelmistoista. Uudet virustorjuntaohjelmat ovat yksinkertaisia asentaa ja saada toimintakuntoon, eivätkä ne vaadi käyttäjältään yleensä toimenpiteitä ohjelman ylläpitoon. Uuden virustorjuntaohjelman asentaminen nostaa tietoturvan tasoa uusilla ominaisuuksillaan ja kuormittaa tietokonetta vähemmän kuin vanhat virustorjuntaohjelmistot. Ohjelmien päivitykset tuovat mukanaan uusien virusten tunnistetietoja, joiden avulla ohjelma pystyy tunnistamaan ja tekemään tarvitut toimenpiteet. Uusissa virustorjuntaohjelmistoissa on myös hyödyllisiä lisäominaisuuksia, kuten roskapostisuodattimet ja vertaisverkkojen sekä pikaviestimien taustasuojaukset. Kyseiset lisäominaisuudet auttavat tietoturvan ylläpidossa muussakin kuin tavallisessa internetin käytössä. Edistyneemmät virustorjuntaohjelmat sisältävät asetuksissaan myös erilaisia tietoturvan tasoja. Virustorjuntaohjelmien asetuksia voidaan muuttaa omien käyttötarkoituksien mukaisiksi ja eri tietoturvaalueiden turvallisuusastetta voidaan tarvittaessa nostaa tai laskea oman mielensä mukaisiksi.

Vaikka virustorjuntaohjelmat ovatkin erittäin tarpeellisia tietoturvauhkien torjunnassa ja poistamisessa, aiheuttavat ne myös monia ongelmia tietokoneen käyttäjille. Sopivan virusohjelman löytäminen tietokoneen teknisiin ominaisuuksiin nähden on vaikeaa ja väärä ohjelma voi hidastaa käyttöjärjestelmän sekä tietokoneen käyttöä. Näissä tapauksissa käyttäjä usein poistaa virustorjuntaohjelmiston tietokoneeltaan ja saattaa ottaa sen pois käytöstä jopa kuukausiksi. Aloittelevat tietokoneiden käyttäjät eivät välttämättä osaa valita sopivaa virustorjuntaohjelmaa, eivätkä tiedä mitä tehdä tartunnan tapahtuessa. Aloittelijalle paras vaihtoehto virus-

torjuntaohjelmistojen kannalta on ostaa internetliittymän mukana sopiva ja helppokäyttöinen virustorjuntaohjelmisto, joka hoitaa kaiken käyttäjän puolesta ja jonka käyttöön saa apua internetoperaattorilta suomen kielellä.

Virustorjuntaohjelmistojen huonoja puolia ovat niinsanotut väärät virusuhkat. Virusohjelma voi tunnistaa täysin turvalliset tiedostot vaarallisiksi ja poistaa ne tietokoneen kiintolevyltä. Edistynyt käyttäjä voi löytää tiedostot virusohjelman karanteenista, josta hän voi palauttaa ne takaisin alkuperäiseen tiedostopolkuun. Käyttäjä joutuu tässä tapauksessa asettamaan virustorjuntaohjelman asetuksista tiedoston turvallisten tiedostojen listalle, jotta ohjelma ei enää välitä tiedoston olemassaolosta ja hälytä kiintolevyllä sijaitsevasta tiedostota uudestaan. Väärät virusuhkat voivat olla myös virusohjelmiston tekijän koodivirhe ja aiheuttaa suuria ongelmia poistaen tietokoneelle tai virustorjuntaohjelmiston toiminnalle tärkeitä tiedostoja ja altistaa toiminnallaan tietokoneen vakaville tietoturvauhkille.

Virukset voivat toiminnallaan tuhota tai häiritä virustorjuntaohjelmien toimintaa. Monet virukset ovat tehty vahingoittamaan tiettyjä virustorjuntaohjelmistoja. Myös virustorjuntaohjelmistoissa on vahingossa aiheutettuja tietoturva-aukkoja, joita hakkereiden on helppo käyttää hyväkseen. Virus voi myös asettaa ohjelmalle uudet valheelliset virustietokannat, jotka eivät estä virusten tartuntaa, vaan kutsuvat toiminnallaan lisää tietoturvauhkia tietokoneelle. Uudet virustorjuntaohjelmat ovat kuitenkin tässä suhteessa erittäin turvallisia ja ohjelmistoille tähdättyjä viruksia tavataan harvoin.

Virustorjuntaohjelma toimii skannaamalla eli se selaa tietokoneen tiedostot läpi, etsien tietoturvauhkia ja poistaen uhkan löytäessään sen. Skannauksen aikana virustorjuntaohjelmisto etsii jälkiä viruksesta tunnistetietokannan avulla. Skannauksen voi käynnistää milloin tahansa tai sen voi asettaa automaattiseksi, jolloin skannaus tapahtuu tietyin väliajoin tiettyyn aikaan. Virustorjuntaohjelmistot eivät aina tunnista tarttuvaa tai tarttunutta tietoturvauhkaa ja tällöin skannaaminen on paras keino löytää tarttuneet aktiiviset ja lepäävät tietoturvauhkat. Skannauksen voi tehdä tarvittaville kohteille erikseen, eikä kiintolevyä tarvitse käydä kokonaan läpi kerralla. CD- tai DVD-asemassa olevat levyt, muistitikut ja muut tietokoneeseen liite-

tyt tiedostoja sisältävät laitteet voidaan skannata erikseen tarvittaessa. Viruksen taustavalvonta suojaa tietokonetta aktiivisesti ja valvoo tietokoneen dataliikennettä analysoiden kiintolevylle tallennetut kohteet. Virustorjuntaohjelmiston päivitys antaa taustavalvonnalle uusimmat tunnistetiedot juuri löytyneistä tietoturvauhkista. Osa virustorjuntaohjelmistoista käyttää heurestista valvontaa, joka tutkii ohjelmistojen epänormaalia toimintaa. Taustavalvonta auttaa käyttäjää havaitsemaan tietokoneelle tarttuvat tietoturvauhkat. Sen avulla käyttäjä ryhtyy helposti toimenpiteisiin tietoturvauhkan leviämistä ja seurauksia varten. Taustasuojausominaisuus on välttämätön internetin käyttäjälle. Taustasuojauksen sisältävän virustorjuntaohjelman asentaminen on erittäin suositeltavaa. Ilman taustasuojausta tietokone on alttiina tietoturvauhkille, vaikka virustorjuntaohjelmisto olisikin asennettuna tietokoneelle. Taustasuojauskaan ei välttämättä ehdi huomata viruksen tarttumista, joten automaattinen tai manuaalinen kiintolevyn tiedostojen skannaus on suoritettava ainakin kerran viikossa. (Symantec 2010.)

4.2 Palomuuri

Palomuuri suojaa tietokonetta rajoittamalla ja estämällä ei-toivottua tietoliikennettä verkosta tietokoneelle ja tietokoneelta verkkoon. Se vahtii porttien liikennettä ja pysäyttää jokaisen sisäänpyrkivän IP-paketin. Jokainen sisääntuleva ja ulosmenevä paketti tarkastetaan huolellisesti, jonka jälkeen se voi jatkaa matkaa määränpäähänsä. Palomuurilla voidaan suojata ulospäin suuntautuvaa liikennettä. Liikenteen turvallisuustasoa saa muutettua oman tarpeen mukaiseksi tarvittaessa, mutta tason muuttaminen on tietoista tietoturvan laiminlyöntiä. Palomuurilla voidaan estää vaarallisilla ja epäeettisillä internetsivuilla vierailua kaikilta tietokoneen käyttäjiltä. Palomuurit eivät kuitenkaan suojaa kaikilta tietokoneelle tulevilta hyökkäyksiltä. Ne eivät myöskään puutu dataliikenteen sisältöön, joten itse haittaohjelmia palomuurilla ei voi estää, mutta hyökkäyksien ja hakkereiden tuomia tietoturvauhkia se pystyy pysäyttämään, huomaamalla ylimääräisen tietoliikenteen. (TKK. 2000. Viestintävirasto 2007.)

Palomuuri on tarpeellinen kotitietokoneissa, jotka ovat yhteydessä internetiin laaja-

kaistayhteyden kautta. Kotikoneet ovat päällä pitkiä aikoja ja näkyvät internetissä samalla IP-osoitteella useita tunteja tai päiviä. Hakkerit kiinnostuvat tietokoneista, joiden IP-osoite pysyy pitkään samana. He murtautuvat niihin tiedostojen tai levytilan vuoksi. Tiedostoja saatetaan varastaa ja käyttää omaksi hyödykseen, mutta useimmiten hakkerit käyttävät tietokoneen kiintolevyn ja verkon kapasiteettia hyökkäysvälineenään. Palveluihin kohdistuvien hyökkäysten lisäksi palomuuri tyypillisesti estää useita erilaisia reititys- ja lähdeosoitteen väärennykseen perustuvia hyökkäystapoja. (Jansson 2010.)

Windows-käyttöjärjestelmä sisältää oman käyttökelpoisen palomuurinsa, mutta tarvittaessa tietoturvaa voi vahvistaa lataamalla muun palomuuriohjelman tai ostamalla erillisen palomuurilaitteen. Yleensä pelkkä käyttöjärjestelmän palomuuri riittää, mutta edistyneet käyttäjät valitsevat myös muita vaihtoehtoja tietokoneensa palomuuriksi. Palomuuri voi tulla myös virustorjuntaohjelmiston mukana ja silloin ylimääräisellä palomuurilla voi olla heikentävä vaikutus Windows-käyttöjärjestelmän omaan palomuuriin. Tässä tapauksessa toinen palomuureista on otettava pois päältä.

Vaikka palomuuri onkin erittäin hyödyllinen ja hyvä ase tietoverkon kautta tulevia hyökkäyksiä vastaan, sen turvallisuustasoa ei kannata asettaa liian korkeaksi eikä liian matalaksi. Liian korkea turvallisuustaso estää tai häiritsee hyödyllisen dataliikenteen kulkua verkossa, aiheuttaen ongelmia esimerkiksi tietoturvaohjelman päivityksien lataantumiselle ja tavalliselle tietoverkossa tehtäville toimille. Liian matala turvallisuustaso sensijaan on tietoturvariski ja altistaa tietokoneen erilaisille hyökkäyksille.

Edistyneet tietokoneen käyttäjät avaavat portteja tarvitsemiaan ohjelmia tai tiedoston jakoa varten. Tämä on tietoturvariski, johon palomuuri ei voi auttaa, ja tietokoneen tietoturva on jatkuvasti uhattuna. Porttien avaaminen on joissain tapauksissa miltei pakollista ohjelmien toiminnan kannalta ja käyttäjä syyllistyy tietoisesti inhimilliseen tietoturvan laiminlyöntiin. Porttien avausta voi välttää vain välttämällä itse ohjelmia, jotka vaativat porttien avausta toimiakseen.

Vain 1 prosentti kaikista palomuurin ilmoittamista hyökkäyksistä on todellisia. Portin kautta hyökkäävän tietoturvauhkan tunnistaa hyökkääjän tutkimista porttinumeroista. Jos hyökkäyksiä tehdään samoihin portteihin tai suureen määrään portteja, kannattaa palomuurin ilmoituksiin kiinnittää huomiota ja ryhtyä tarvittaviin toimenpiteisiin. Palomuurin lokitiedostoista voi tarkistaa hyökkäyksen vakavuuden ja mitä porttia hyökkäykset ovat koskeneet. Avonaisia tai tietoturva-aukkojen vuoksi avautuneita portteja voidaan joissain tapauksissa sulkea itse. Hyökkäyksen kohteena olleen tietokoneen käyttäjä voi etsiä lisätietoa porteista ja niiden suojauksesta internetistä. Palomuurin, kuten virustorjuntaohjelmienkin, ilmoitukset eivät tarkoita tietoturvauhkan tunkeutumista tietokoneelle, vaan se voi ilmoittaa myös estäneensä hyökkäyksiä. Esimerkiksi trojan-haittaohjelman tekijä voi yrittää ottaa yhteyttä saastuneeseen tietokoneeseen haluaminsa porttien avulla. (Jansson 2010.)

4.3 Internetselainten tietoturva

Internetselaimet ovat kehittyneet vuosien saatossa turvallisemmiksi ja suhteellisen luotettaviksi käyttää. Selaimia kehitetään jatkuvasti ja niiden ohjelmakoodi joutuu muunnoksen kohteeksi monta kertaa vuodessa. Tämä jättää koodiin useita tietoturva-aukkoja, joita internetrikolliset pääsevät helposti hyödyntämään omiin tarkoituksiinsa. Tietoturva-aukkojen synty on tietoturvan inhimillinen uhkatekijä, johtuen koodin kirjoittajan huolimattomuudesta.

Eniten ongelmia tietoturva-aukkojen alueella on ollut Microsoftin Internet Explorer-internetselaimessa. Internet Explorer on maailman käytetyin internetselain (Kuvio 1), johtuen Windows-käyttöjärjestelmästä, joka asentaa käyttäjälleen oletusselaimeksi ilmaisen Internet Explorer -ohjelman. IE on aiheuttanut monia virustartuntoja oman koodinsa tietoturva-aukkojen vuoksi eikä kaikkia ongelmia ole saatu vuosien saatossa korjattua kokonaan, vaikka selaimesta on tullut monia uusia versioita. Internet Explorer sisältää myös lisäosan, ActiveX:n, jolla voi liittää selaimeen ActiveX- tekniikkaa käyttäviä komponentteja. Tuntemattomien ja haitallisten ActiveX-komponenttien lataus altistaa tietokoneen tietoturvauhkille. (Kotilainen 2.3.2010.)

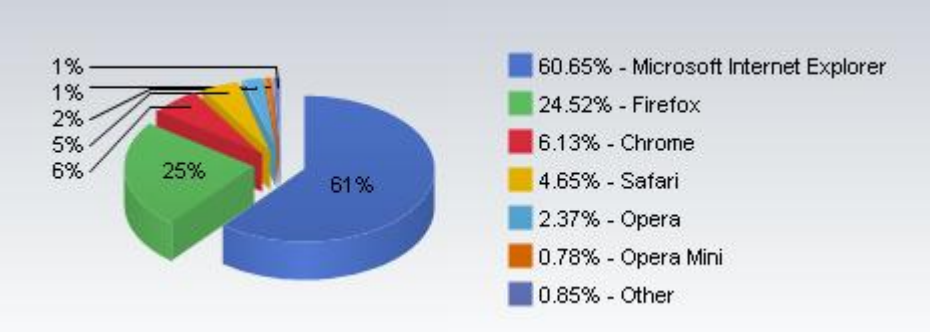
Myös muihin selaimiin, kuten Mozilla Firefoxiin on kehitetty lisäosia, mutta yksikään lisäosa ei ole ollut yhtä suuri tietoturvariski kuin ActiveX- komponentti. Mozilla Firefox-selaimen lisäosat ovat päinvastastaisesti edistäneet tietokoneiden tietoturvaa. Selain antaa käyttäjälleen mahdollisuuden ladata erillisiä lisäosia, jotka tunnistavat vaaralliset ja epäluotettavat internetsivut suosituissa hakukoneissa. Myös mainostenesto-ohjelmat, kuten Ad-Block Plus, estävät käyttäjää painamasta haitallisia mainoksia ja linkkejä, jotka voivat johtaa vakaviin seurauksiin henkilökohtaisten tietojen menetyksinä. Suurin uhka internetselaimia käytettäessä on oman tiedon huolimaton jakelu, laittomien tiedostojen lataus, sähköpostin liitetiedostojen avaus, epäeettisillä sivustoilla vierailu sekä muille internetiä käyttäville henkilöille tehty haitta. Internetselaimen tuoma turva ei riitä, jos käyttäjä syyllistyy jatkuvasti tietoturvan laiminlyöntiin.

Valitettavasti yksikään internetselain ei ole täysin turvallinen. Internet Explorer- selaimen vaihtoehdoksi asetettu Mozilla Firefox koki myös tietoturva-aukon haitallisen vaikutuksen maaliskuussa 2010. Myös suosiota kasvattavat Google Chrome ja Safari ovat joutuneet tietoturva-aukkojen haittavaikutusten kohteeksi. Mozilla Firefox-selaimen versio 3.6 sisälsi tietoturva-aukon, joka sai useat käyttäjät pohtimaan oman selaimensa turvallisuutta, kun selain kaatui helposti jopa peruskäytössä. Uusi Google Chrome selain on testattu turvallisimmaksi ja nopeimmaksi Windows- käyttöjärjestelmän internetselaimeksi, joskin sen mukana tulevat ominaisuudet ovat hyvin heikkoja verrattuna laajemmin levinneisiin kilpailijoihinsa. (Cert-fi 30.3.2010.)

Uusin Internet Explorer 9-selain on huomattavasti turvallisempi vaihtoehto, kuin selaimen versiot 6, 7 ja 8. Jopa Saksan valtio on varoittanut kyseisten selainten haavoittuvaisuuksista ja kehoittanut internetin käyttäjiä päivittämään Internet Explorerin versioon 9 tai vaihtamaan internetselaimensa toiseen selaimeen. (Emery 2010.) Valitettavasti Internet Explorer- selain ei ole internetin käyttäjälle ilmainen ja ladattavissa oleva, ellei omista Windows-käyttöjärjestelmän käyttöoikeutta. Tämän seikan vuoksi monet internetpalveluiden tarjoajat ovat lopettaneet tukensa vanhoja selainversioita käyttäville henkilöille, sillä niitä ei voi päivittää uudempiin versioihin vanhoissa käyttöjärjestelmissä. Tietokoneen ja internetin käytön aloittelija käyttää

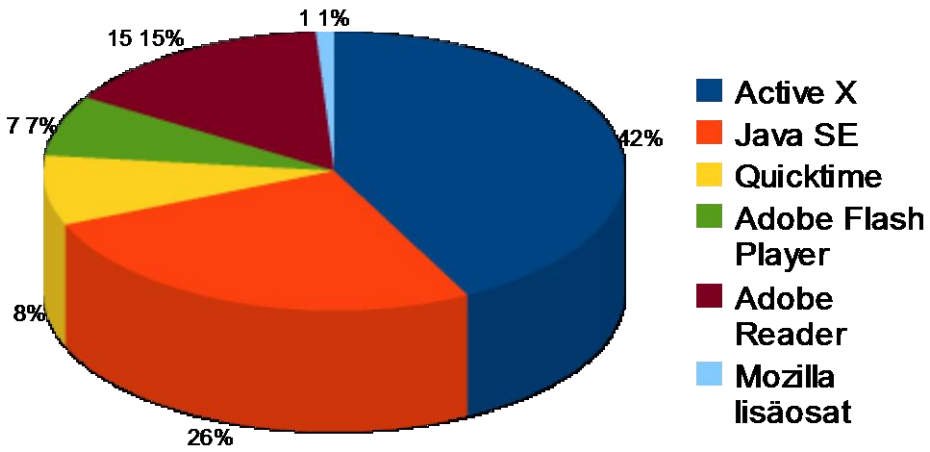
juuri näitä vanhoja selainversioita ja levittävät tietoturvauhkia tietämättä internet-selaimen haavoittuvaisuuksista mitään.

Paras vaihtoehto vaihtaa turvalliseen internetselaimeen on asentaa joko Mozilla Firefox, Google Chrome tai Opera tietokoneen käyttöjärjestelmälle. Kaikki näistä selaimista on tietoturvaltaan moninkertaisesti parempia kuin Internet Explorer ja käyttöjärjestelmältään jopa lopulta helppokäyttöisempiä ja nopeampia. Tietokoneen tietoturvaa voi nostaa huomattavasti vaihtamalla internetselaimen kokonaan uuteen ohjelmaan tai päivittäessä vanhan selaimen uuteen versioon. Internet Exploreria ei suositella käytettäväksi päivittäisessä internetin käytössä ja käyttäjiä suositetaan vaihtamaan Mozilla Firefox-internetselaimeen. Vanhoja selainversioita ei kehoiteta käytettäviksi, sillä mitä pidempään selainversio on vapaassa käytössä, sitä enemmän rikolliset voivat löytää ja hyödyntää sen tietoturva-aukkoja. (Kotilainen 20.4.2010.)



Kuvio 1. Internetselainten käyttö prosentteina huhtikuussa 2010. Lähde: Net Applications 2010.

Internet Explorer on haavoittuvaisuuksistaan huolimatta maailman käytetyin internetselain. Sen käyttöprosentti on kuitenkin laskusuhdanteessa muiden ominaisuuksiltaan ja tietoturvaltaan parempien internetselainten suosituksen kasvaessa (Kuvio 1).



Kuvio 2. Internetselainten suurimmat haavoittuvaisuudet 2009. Lähde: Symantec 2010.

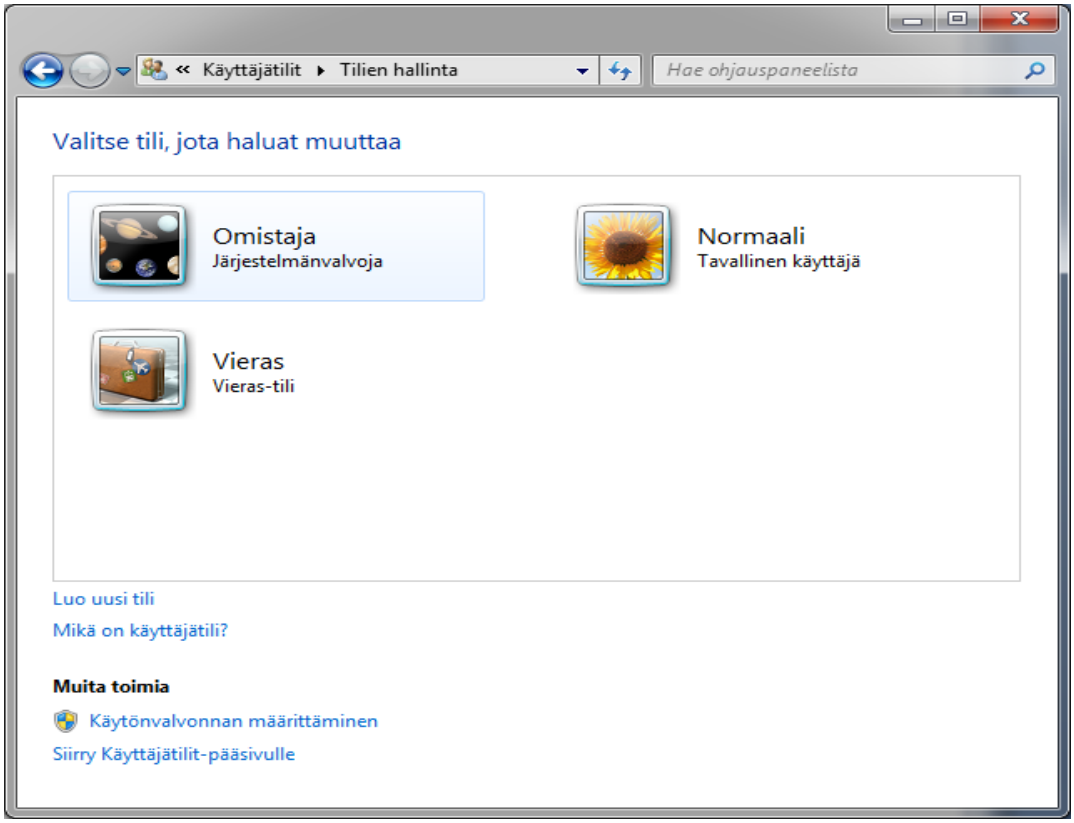
Symantec- yhtiön tekemän tutkimuksen mukaan jopa 42- prosenttia eli 134 kappaletta erillisiä haavoittuvaisuuksia liittyy Internet Explorer- internetselaimen ActiveX- komponenttiin. Toinen erittäin huomattava haavoittuvaisuus koskee myös Internet Explorerin ActiveX- komponenttia. ActiveX:n toimintaan liittyvä ohjelmointikieli Java SE sisälsi 26- prosenttia, eli 84 haavoittuvaisuutta. Muut mainittavat haavoittuvaisuudet koskevat Adobe Reader- , Quicktime- ja Adobe Flash Player- ohjelmia, jotka vaikuttavat kaikkien internetselaimien turvallisuuteen. Näistä tutkimustuloksista voidaan huomata suurimmat internetselaimia koskevat uhat ja tunnistaa Internet Explorer- selaimen turvallisuuden heikoksi. Ainoastaan Mozilla Firefoxia haittaavia haavoittuvaisuuksia löydettiin vain neljä kappaletta, mikä on yli 80 kertaisesti pienempi, kuin Internet Explorer- selainta koskevien uhkien määrä (Kuvio 2).

4.4 Windows- käyttöjärjestelmän käyttäjävalvonta

Tietokoneiden käyttäjien ei aina kannata avata käyttöjärjestelmää järjestelmänvalvojan tunnuksella ja salasanalla. Käyttöliittymän käyttö käyttäjätilillä (Kuvio 3), jolla ei ole lupaa muuttaa ohjelmien tietoja, on tietokoneen peruskäyttäjälle turvallinen vaihtoehto, sillä kaikki tietoturvauhkat eivät voi levitä ja tehdä muutoksia

tietokoneen järjestelmälle alhaisemmilla käyttäjätilien tasoilla. Tietokoneen käyttäminen muulla kuin järjestelmänvalvojan tunnuksilla on siis hyvin suotavaa sellaisessa käytössä jossa ohjelmien asennus ei ole päivittäistä ja käyttöjärjestelmään tehdään hyvin vähän muutoksia. Käyttäjätilin tyyppi antaa käyttäjälle eri tasoiset tietokoneen käyttö- ja valvontaoikeudet. Käyttäjätiliä on kolmea eri tasoa. Normaali käyttäjätili on hyvä päivittäiseen käyttöön, sillä voidaan tehdä töitä normaalisti, mutta käyttöjärjestelmään tehtävät muutokset eivät ole mahdollisia. Tiliä kannattaa käyttää tietoturvan vuoksi, sillä haittaohjelmatkaan eivät voi tehdä laajoja muutoksia tietokoneen käyttöjärjestelmään.

Järjestelmänvalvojan tili antaa käyttäjälleen oikeudet tehdä kaiken mitä hän haluaa. Tätä tiliä tulisi käyttää vain harvoin, silloin kun tietokoneen ohjelmistoja tarvitsee päivittää tai asentaa tai silloin kun järjestelmän tietojen tarkastelu ja muuttaminen on ajankohtaista. Kolmas tili, Vieras, on sopiva tili tietokonetta harvoin käyttäville tai tietokoneen käytön huonommin hallitseville henkilöille, joilla ei tarvitse olla pääsyä kaikkiin ohjelmiin tai kansioihin. Vierastili ei sovellu tietokonetta joka päivä käyttäville henkilöille, sillä tilin turva-asetukset voivat olla käyttäjälle liian korkeita.



Kuvio 3. Esimerkki Windows 7-käyttöjärjestelmän käyttäjätileistä.

4.5 Salasanat

Salasanan avulla henkilökohtaisen tiedon varastaminen on vaikeampaa ja tietokoneelle tai palveluihin tunkeutumisen uhka vähentyy. Salasana kannattaa pitää monimutkaisena ja vaikeana, mutta salasanaa ei saa jättää muiden henkilöiden näkyville tai tietoon. Salasanojen arvailuun on kehitetty monia ohjelmia, jotka yrittävät arvata oikean salasanan. Jos salasana on tarpeeksi vaikea, ohjelmat eivät pysty arvaamaan oikeaa salasanaa ja tietoturva on suojattu paremmin.

Monet sähköpostien käyttäjät käyttävät liian yksinkertaista ja arvattavaa salasanaa. Liian helppo salasana on tietoturvan laiminlyöntiä ja se kannattaa muuttaa vaikeampaan salasanaan. Myös pankkitunnusten ja muiden tärkeiden salasanojen tallentaminen tietokoneen muistiin ei ole suositeltavaa trojaneiden ja keylogger haittaohjelmien vuoksi.

Salasanan pituuden kannattaa olla vähintään 10 merkkinen, mutta mielellään yli 14- merkkinen. Sen on sisällettävä isoja sekä pieniä kirjaimia, symboleja sekä numeroita. Jos salasana sisältää liian monta samanlaista merkkiä, se kannattaa tehdä hyvin pitkäksi. Samaa salasanaa ei saa käyttää eri järjestelmissä ja vaikeatkin salasanat täytyy vaihtaa sopivin väliajoin. Paras salasana on palvelusta riippuen mahdollisimman pitkä ja se sisältää useita erilaisia symboleita, eikä muodosta minkäänlaista sanaa, jonka voi löytää esimerkiksi tietosanakirjan sivulta. Internetissä on salasanantarkistin ohjelmia, joilla voi tarkistaa salasanansa vahvuuden ja muokata ohjelman avulla salasanansa tietoturvaltaan paremmaksi. Suurimmat virheet on käyttää salasanana password- tai salasana- sanaa ja yksinkertaisia numeroyhdistelmiä kuten 1234.

Valittua salasanaa ei saa tallentaa mihinkään, ei tekstiasiakirjaan, paperilapulle tai selaimen tietoihin. Se kannattaa vain opetella muistamaan ulkoa, jolloin voidaan välttää inhimillisen tietoturvauhkan toteutumisen. Jos salasanasta haluaa jättää jonkinlaisen muistutuksen, kannattaa se kirjoittaa muistiin sellaisena, ettei sitä voi ymmärtää salasanaksi tai suojata sen huolellisesti tekstinkäsittelyohjelman suojauksella. Paperilappu on turvallisempi salasanan muistutustapa kotikäyttäjälle, kuin tiedostoon tallentaminen, mutta yrityksille paperilapulla olevat salasanat ovat erittäin suuri tietoturvauhka. (Microsoft 2006.)

1. 123456
2. 12345
3. 123456789
4. password
5. iloveyou
6. princess
7. rockyou
8. 1234567
9. 12345678
10. abc123

Kuvio 4. Eniten käytetyt, tietoturvaltaan huonot salasanat. Lähde: Impreva 2010.

Yksi viidestä internetin käyttäjästä valitsee heikon ja helposti arvattavan salasanan. Imperva teknologia yrityksen teettämän tutkimuksen mukaan, jossa he kävivät läpi 32 miljoonan salasanan hakkeroitua listaa, yleisimmät salasanat ovat 123456, 12345, 123456789 ja password (Kuvio 4).

Hyvä salasanakaan ei välttämättä auta sähköpostitilin suojaamiseen, sillä sähköpostipalveluntarjoajien turvakysymysrutiinit ovat usein liian heikkoja. Tähän on tulossa pian muutoksia useiden sähköpostipalveluiden tarjoajilla ja salasanojen vaatimukset muuttuvat tietoturvan kannalta paremmiksi. (Karkimo 9.3.2010.)

5 HAITTAOHJELMIEN PUHDISTAMINEN JA POISTO

Miten tietoturvauhkan tarttumisen tietokoneelle yleensä huomaa? Tartunnan huomaa joskus helposti, mutta osa tietoturvauhkista voi pysyä näkymättömissä kauankin aikaa. Erilaiset virustorjuntaohjelmistot ja palomuuriratkaisut voivat huomata haittaohjelman tartunnan tai mahdollisen hyökkäyksen estäen sen tai ilmoittaen siitä erillisellä ikkunalla. Virustorjuntaohjelmistot ilmoittavat tartunnasta tartunnan tunnistamisen aikana, mutta varoitusikkunat eivät näy ruudulla kovin kauaa. Käyttäjältä tartunta voi siis jäädä huomaamatta ja virustorjuntaohjelman epäonnistunut tartunnan puhdistaminen saattaa jättää tietoturvauhkan tietokoneen kiintolevylle.

Tietoturvauhkan aiheuttamat seuraukset ovat usein näkyviä. Internetin käytön huomattava hidastuminen on ensimmäisiä tartunnan merkkejä. Haittaohjelman tartunnan huomaa helposti myös tietokoneen toiminnan hidastumisena, käyttöjärjestelmän toiminnan häiriintymisenä, tiedostojen katoamisina, asetuksien muunnoksina, tunnistamattomien sähköpostien lähetyksinä ja uusien ohjelmien ilmestymisenä. Internetin hidastumisen tuntee käyttäessään internetselainta ja käyttäjän vierailessa erilaisilla internetsivuilla. Internetsivujen on lataus on tällöin hidasta tai ne eivät lataudu ollenkaan, sivustoja uudelleenohjataan väärille ja haitallisille sivustoille, kotisivu ja internetselain kaapataan tai internet tuntuu muuten vain entistä hitaammalta. Usein sivustojen uudelleenohjautuminen ja selaimen täydellinen kaappaus ovat häiritseviä ja huomiota herättäviä tartuntojen seurauksia. Näissä tapauksissa käyttäjä joutuu hämilleen, ehkä jopa paniikkiin, eikä tiedä mitä voisi tehdä tartunnan poistamiseksi. (Jansson 2010.)

Tartuntoja varten tietokoneella tulisi olla päivitetty, mielellään heurestinen virustorjuntaohjelmisto ja spy- ja adware haittaohjelmia poistavia ohjelmistoja. Nämä erilliset ohjelmat toimivat paremmin vakoilu- ja mainosohjelmia vastaan, kuin tavallinen virustorjuntaohjelmisto. Joissain tapauksissa virustorjuntaohjelmisto voi olla kaapattu ja ainoa mahdollisuus tietoturvauhkan poistamiseksi on käyttää tai asentaa uusi haittaohjelmien poisto-ohjelma.

Kun käyttäjä tietää tartunnasta, hänen kannattaa ensimmäisenä kytkeä tietokone

pois internetistä irroittamalla internetkaapelin tietokoneestaan tai sulkemalla langattoman internetyhteyden. Haittaohjelmien poisto aloitetaan tyhjentämällä tietokoneen temporary files (tmp / temp) kansiossa sijaitsevat tiedostot. Välimuistikansiossa sijaitsevat haittaohjelmat voidaan parhaimmassa tapauksessa saada poistettua erittäin yksinkertaisesti, käyttämällä käyttöjärjestelmän tiedostojen poistotoimintaa. Jos välimuistikansiossa oleva haittaohjelma käyttää aktiivisesti tietokoneen muistia, sitä ei saa poistettua ilman prosessien kiinnilaittoa tai vikasietotilassa toimintaa.

Seuraavaksi käyttäjän täytyy aloittaa tietokoneen kiintolevyn haittaohjelmien etsintä eli skannaus, jotta kaikki tietoturvauhkat löytyvät ja tietoturvaohjelma voi puhdistaa löydetyt tartunnat. Tietoturvaohjelman skannaus kannattaa suorittaa vikasietotilassa, jolloin kaikki normaalisti käynnissä olevat palvelut ja prosessit eivät ole käytössä. Jos käyttöjärjestelmälle tärkeään tiedostoon on tarttunut virus, sen poistaminen voi olla mahdotonta ilman vikasietotilassa toimintaa. Kun skannaus on päättynyt ja tietoturvaohjelma on löytänyt tietoturvauhkia, uhkat poistetaan tietokoneen kiintolevyltä karanteeni kansion kautta. Poistamisen jälkeen virustorjuntaohjelman skannaus suoritetaan uudestaan, koska tietyt haittaohjelmat on suunniteltu asentamaan itsensä uudelleen mahdollisen poiston jälkeen. Jos ohjelma löytää samat tartunnat toisella tarkistuskerralla, täytyy ryhtyä uusiin toimiin tietoturvauhkien poistoa varten. Skannausta kannattaa kokeilla myös muilla kuin yhdellä virustorjuntaohjelmistolla ja käyttää internetissä olevia online-skannereita kuten Kaspersky, Housecall ja F-secure. Monissa tapauksissa tietoturvauhka sotkee internetselaimen toimintaa niin paljon, että internetissä toimivia ohjelmia on mahdotonta käyttää. Tietokoneella ei saisi kuitenkaan olla asennettuna enemmän kuin yksi virustorjuntaohjelma, koska ne voivat häiritä toistensa toimintaa ja vaikuttaa tietokoneen käyttöön negatiivisesti, hidastaen konetta ja estäen verkkoliikennettä. Tämän vuoksi internetissä toimivien virus-skannerien käyttö on toivottavaa viruksia poistaessa. (Jansson 2010.)

Kun virustorjuntaohjelmien tuoma apu ei riitä tai niitä ei voi tartunnan vuoksi käyttää, tarvitaan tartuntaa vastaan lisäohjelmia tai manuaalista poistamista käyttäen Windows- käyttöjärjestelmän rekisteritiedostojen editointi ohjelmaa ja resurssienhallinnan tiedostojen etsintää. Joskus haittaohjelman saastuttaneita tiedostoja voi olla hyvin vaikea poistaa. Tässä tapauksessa manuaalinen poisto voi olla ainoa tapa saada haittaohjelma pois tietokoneelta. Jos haittaohjelma ei lähde tietokoneelta tiedostojen manuaalisella tai ohjelman avulla poistamisella, eikä käyttäjä tiedä mitä voisi tehdä käyttöjärjestelmän pelastamiseksi, tulee hänen kysyä apua internetistä, internet operaattorilta tai virustorjuntaohjelmiston help-desk puhelimesta.

Internetissä on monia tietoturvauhkiin perehtyneitä keskustelupalstoja, joiden jäsenet auttavat haittaohjelmien kanssa kamppailevia tietokoneiden käyttäjiä. Ennen kuin käyttäjää voidaan auttaa, joutuu hän lähettämään keskustelupalstalle HiJackThis- ohjelman loki tiedoston, joka kertoo mitä aktiivisia prosesseja ja palveluita käyttäjän tietokone sisältää. Näiden lokitiedostojen avulla, keskustelupalstan jäsenet voivat auttaa käyttäjää valitsemaan oikeat ohjelmat ja menetelmät haittaohjelman poistamista varten. HiJackThis- ohjelman lokitiedostot voidaan myös lähettää suoraan ohjelman tekijän internetsivulle, jossa loki analysoidaan ja josta selvitetään mitä prosesseja ja palveluita käyttäjä voi turvallisesti korjata HiJack-This-ohjelman avulla. Käyttäjä voi myös itse analysoida mahdollisia tietoturva-uhkia internetsivulta löydettävällä HiJackThis Online Analysator- ominaisuudella.

Löytyneitä haittaohjelmia varten tarvitaan usein niihin erikoistuneita poisto-ohjelmia. Tälläisiä ohjelmia ovat 32- bittiselle Windows- käyttöjärjestelmille tehty Combofix ja ohjelmat SpyBot Search And Destroy, Malwarebytes Anti-Malware, Ccleaner, SuperAntiSpyware ja Ad-Aware. Kaikki yllämainitut ohjelmat ovat ilmaisia ja ladattavissa suomalaisilta internetsivuilta, mutta kaikki eivät ole suomenkielisiä. Peruskäyttäjä voi joutua pyytämään apua ohjelmien käytössä, eikä varsinkaan Combofix- ohjelmaa saa käyttää ilman asiaan perehtyneen opastusta. Muut yllämainitut erikoisohjelmat ovat helppoja asentaa ja käyttää, eikä niiden toimintaan tarvita erityistä neuvoa.

Jos haittaohjelmaa ei saa puhdistettua manuaalisesti, ohjelmalla tai internetistä saadulla avulla, täytyy tietokoneen käyttäjän pahimmassa tapauksessa asentaa käyttöjärjestelmä kokonaan uudelleen. Saastuneiden tiedostojen pois saamiseksi tietokoneen kiintolevy tulee alustaa, jolloin käyttäjä menettää kaikki tietokoneella sijaitsevat tiedostot. Saastuneesta tietokoneesta ei saa ottaa tiedostoja talteen, eikä tehdä varmuuskopioita, sillä haittaohjelma voi tartuttaa itsensä melkein jokaiseen tiedostomuotoon, erityisesti käyttöjärjestelmälle tärkeisiin tiedostoihin. Joskus järjestelmän palautus- toiminto saattaa auttaa haittaohjelman poistamiseksi, mutta heti tartunnan tapahduttua järjestelmän palautus toiminto on laitettava pois päältä. Jos järjestelmä tekee palautuspisteen saastuneesta käyttöjärjestelmästä, tietokonetta voi olla mahdoton puhdistaa kyseisellä menetelmällä. Monet tietoturvauhkat käyttävät koodiaan järjestelmän palautus toimenpiteen estämiseksi. Näissä tapauksissa vanhaan palautuspisteeseen palaaminen on hyödytöntä ja joissain tilanteissa mahdotonta.

Kun haittaohjelman vakavuus ja sen aiheuttamat seuraukset ovat käyttäjän tiedossa ja kaikki keinot sen poistamiseksi on kokeiltu, täytyy tietokoneen kiintolevy alustaa. Tämä on aloittelevalle tietokoneen käyttäjälle liian vaikeaa, eikä kiintolevyä tulisi alustaa ellei tiedä mitä on tekemässä ja omista käyttöjärjestelmän asennuslevykkeitä. Tässä tapauksessa kiintolevyn alustus kannattaa jättää lähimmän atk- huollon työksi tai kokeneemmalle tietokoneen käyttäjälle.

6 JOHTOPÄÄTÖKSET

Haittaohjelmien leviämis- ja esiintymistilanne pahenee tulevaisuudessa, sillä ammattirikolliset tekevät viruksia harrastajia enemmän. Virusten vakavuus kasvaa ja ne voivat vaikuttaa ihmisten elämään maan tai maailmanlaajuisesti. Virusten näkyvyys heikentyy ja niiden leviäminen helpottuu entisestään, johtaen yhä useamman tietokoneen saastumiseen. Pahenevaa tietoturvan tilaa yritetään kohentaa monilla eri osa-alueilla uusilla teknisillä ratkaisuilla, vaikka vain inhimillisen tietoturvan nostaminen saattaisi osaltaan riittää.

Yksi Microsoft- yhtiön keinoista lisätä tietoturvaa on eristää turvattomat tietokoneet internetistä. Tämän avulla saastuneet tietokoneet eivät voisi tartuttaa toisia tietokoneita internetin välityksellä. Saastunutta tietokonetta täten etähallittaisiin niin, että niistä tehtäisiin turvallisia. Tietokone asetettaisiin karanteeniin, jossa se voidaan puhdistaa etähallittuna tai kehottaa käyttäjää puhdistamaan tietokoneen tietoturvauhkista, ennen kuin hän pääsee takaisin internetiin. Eristäminen koskisi myös tietokoneita, joita ei ole päivitetty ja ovat täten alttiimpia erilaisille tietoturvariskeille. Saastuneelle tai päivittämättömälle tietokoneelle voidaan kuitenkin tarjota rajoitettu ympäristö, jossa tietoturvaongelmat voidaan korjata. Tämä rajoitettu tietoverkon ympäristö estäisi tietoturvauhkien leviämistä ja antaisi käyttäjälle sopivasti aikaa haittaohjelmasta koituvan ongelman ratkaisulle.

Kyseinen keino on vasta idea tasolla, mutta on hyvin mahdollinen ja yksinkertainen toteutettavaksi. Tällä tavoin virusten tarttuminen ja leviäminen sekä laittomien Windows- käyttöjärjestelmien tuomat uhkat minimoituvat. Laittomia Windows- käyttöjärjestelmän versioita olisi vaikeampi käyttää, sillä ne eristettäisiin tietoverkosta kokonaan, vähentäen siis piratismia ja haittaohjelmien levittämistä. (Kotilainen 4.3.2010.)

Lähivuosina tietoturvauhkat sosiaalisessa mediassa, verkkopankeissa ja ohjelmistoissa lisääntyvät, niiden suosion ja yleistymisen myötä. Myös kohdistetut hyökkäykset koti- ja yritystietokoneisiin sekä sisäisiin tietoverkkoihin muuttuvat vaarallisemmiksi. On odotettavissa, että internetrikolliset jäävät kuitenkin myös helpom-

min kiinni ja taistelu haittaohjelmia vastaan kiristyy.

Internetsivustoista Facebook, verkkopankit sekä sähköpostien liitetiedostot ovat yhä suurempi uhka tavalliselle internetin käyttäjälle. Myös Adoben sovellukset Acrobat Reader ja Flash tulevat olemaan rikollisten suosiossa ja todennäköisesti niille tehdyt uhkat ohittavat Microsoft- yhtiön ohjelmistoille tehtyjen uhkien määrän.

Suositut sosiaaliset sivustot, kuten Facebook ja Twitter joutuvat taistelemaan haittaohjelmia vastaan suosion kasvaessa. Suosion kasvu kiinnostaa internetrikollisia ja he suunnittelevat uusia haittaohjelmia, joita tartuttaa helposti jopa miljooniin tietokoneisiin. Kyseisissä palveluissa ei usein varota ystävien lähettämiä tiedostoja tai linkkejä. Palvelua käyttävä ei usko saavansa viruksia turvallisen tuntuisesta palvelusta ja ei saata uskoa tietoturvauhkien mahdollisuutta. Ongelmia tuottaa myös Twitterissä käytettävien URL- osoitteiden vuoksi URL- palvelut, joiden avulla Twitterin käyttäjät tutkivat tapahtuvia uutisia, tapahtumia ja muiden käyttäjien viestejä. Nämä linkit johtavat siihen, että käyttäjä siirtyy tietämättään vaaralliselle sivustolle painamalla harmittoman näköistä URL- osoitetta. Sosiaalisen median internetsivustoja kannattaa siis tulevaisuudessa välttää tai käyttää hyvin harkitusti. Näihin sivustoihin tehdään yhä useampia hyökkäyksiä ja haittaohjelmia. (McAfee 2009.)

Internet sivustojen tekninen muunnos HTML 5- koodin myötä, tuo uudet tietoturvariskit. HTML 5- kieli sumentaa käyttöliittymän ja selaimen rajan, antaen rikollisille uusia keinoja tietokoneiden kaappaamiseksi. Myös uudet käyttöliittymät ja internet selaimet, kuten Google Chrome ja Google Wave tuovat käyttöjärjestelmille uusia ennennäkemättömiä viruksia, jotka voivat tartuttaa ja käyttää tietokonetta helpommin. (McAfee 2009.)

Sähköpostin kautta hyökkäävät tietoturvauhkat yleistyvät entisestään ja rikolliset nimeävät sähköpostit yhä houkuttelevammin. Sähköpostihyökkäykset kohdistuvat tiettyihin osoitteisiin joiden palvelimet on valittu etukäteen. Näitä Botnet- verkkoja, eli tietokoneita jotka ovat yhdistetty tälläisillä sähköposteilla, tutkitaan ja etsitään jatkuvasti. Yleensä nämä tietokoneet ovat hallitusten, avustusjärjestöjen sekä aktivistien käytettävinä. Sähköpostin ja sen liitteiden kautta hyökkäävät tietoturvauhkat

tulevat olemaan ongelma myös useille uutispalveluille ja niiden journalisteille. Tunnetut internetin uutispalvelut ovat miljoonien käyttäjien joka päiväisiä käyntisivustoja ja näillä aloilla on tunnettava erityistä varovaisuutta uutislinkkien ja lisätietojen osoitteiden turvallisuudesta. (McAfee 2009.)

Suurimmat ongelmat lähivuosina tietoturvan näkökulmasta ovat ohjelmistojen haavoittuvaisuudet ja tietoturva-aukot. Rikolliset hyödyntävät haavoittuvaisuuksia yhä helpommin ja trojan- tietoturvauhkat yleistyvät entisestään. Adobe- ja Microsoft yhtiöiden ohjelmistot ovat edelleen uhan alla ja virukset leviävät myös Adoben flash-kielellä tehtyihin ohjelmiin ja sivustoihin. Näitä ohjelmistoja käyttävät henkilöt omistavat usein vanhoja versioita kyseisistä ohjelmista ja tietoturvauhkat leviävät hyvin helposti erityisesti niiden kautta. Flash ja Adobe Reader- ohjelmia ovat erittäin yleisesti käytössä koko maailmassa ja ne ovat kiinnittäneet haittaohjelmien kehittäjien huomion. Adobe tulee pian ohittamaan Microsoft Office ohjelman kautta tehtyjen hyökkäysten määrän. Haavoittuvaisuuksien määrässä Apple- yhtiön sovellukset (Kuvio 5), ovat jo ensimmäisellä sijalla. (IBM 2010.)

Ranking	Vendor
1.	Apple
2.	Sun
3.	Microsoft
4.	IBM
5.	Oracle
6.	Mozilla
7.	Linux
8.	Cisco
9.	Adobe
10.	HP

Kuvio 5. Eniten haavoittuvaisuuksia ohjelmistoissa. Lähde: IBM 2010.

Uusien Internet Explorer versioiden avulla, Windows- käyttöjärjestelmille leviävät haittaohjelmat vähenevät runsaasti. Uusikaan versio ei ole täysin aukoton, mutta turvallisempi vaihtoehto kuin vanhat tutkitusti tietoturvauhkille alttiit selainversiot.

Ennen HTML 5- koodikielen käyttöönottoa, nykyiset käytetyimmät selaimet tulevat saamaan vielä useita tietoturvauhkia, jotka hyödyntävät ohjelman haavoittuvaisuuksia.

Trojan, rootkit ja keylogger tietoturvauhkat yhdistetään toisiinsa ja niistä tehdään uusia entistä vaikeammin huomattavia haittaohjelmia. Trojanit ovat alkaneet käyttää rootkit ominaisuutta, jonka avulla sitä ei voi tunnistaa ja puhdistaa tietokoneelta yksinkertaisilla menetelmillä. Nämä trojanit estävät virustorjuntaohjelmaa lataamasta uusia päivityksiä, jonka vuoksi se ei pysty enää tunnistamaan trojanin mahdollisesti lataamia haittaohjelmia. Trojan keylogger haittaohjelmat yleistyvät ja kehittyvät paremmin naamioimaan itsensä esimerkiksi verkkopankin etusivuksi. Tulemme näkemään monien pankkitilien tyhjentyvän ja rahojen menevän hyökkääjän tilille. Rikollisilla saattaa siis olla rahakkaat päivät edessä ohjelmistojen ja internetpalveluiden haavoittuvaisuuksien yleistyessä.

Yleisille matkapuhelinkäyttöliittymille tehdyt haittaohjelmat yleistyvät, älypuhelinten käytön kasvaessa ja niiden käyttötarkoituksen muuttuessa enemmän internetin selailuun ja sähköpostin tarkistamiseen. Valitettavasti uusien älypuhelinten tietoturva on heikkoa, eikä tietoturvauhkia voida torjua tehokkaasti. Internetselaimen omaaville älypuhelimille tulisi tehdä omia tietoturvaohjelmia ja palomuureja tietoturvallisuuden kasvattamiseksi.

Tietoturvalle on luvassa monia erilaisia haasteita vuonna 2010 ja tulevina vuosina. Uusia teknisiä ja inhimillisiä ratkaisuja keksitään ja suunnitellaan jatkuvasti ja niiden kehityksessä joudutaan olemaan yhä innovatiivisempia. Vaikka tietoverkkojen käytössä halutaan pitää yksityisyys, toimisi isoveli valvoo tyyppinen ratkaisu tietoturvan osalta internetissä mainiosti. Internet on kuitenkin vapaa verkko, eikä sen toimintaperiaatetta tarvitse välttämättä muuttaa. Omat jokaiselle henkilökohtaiset internet-tunnukset olisivat maailmanlaajuisesti merkittävä edistysaskel tietoturvan näkökulmasta. Tunnuksella voitaisiin valvoa käyttäjien haitallisia toimia ja niiden perusteella inaktivoida käyttäjän oikeus internetin käyttöön tietyksi ajanjaksoksi tai mahdollisesti kokonaan.

Tulevaisuuden mahdollisesti yleistyviin tai uusiin tietoturvauhkiin on perehdyttävä tietoturvan säilyttämiseksi. Tämä perehtyminen auttaa tietoverkkojen käyttäjää ennaltaehkäisemään ja tunnistamaan tarttuvien haittaohjelmien tyypit tehokkaasti. Tietoturvan kehitys on riippuvainen inhimillisten tietoturvauhkien vastuun kasvattamisesta maailmanlaajuisella tasolla. Yksittäisten henkilöiden henkilökohtaisen tietoturvan parantaminen on merkittävä osa maanlaajuisen tietoturvan suojaamiselle, eikä sitä kannata laiminlyödä sillä yksi saastunut tietokone voi levittää haittaohjelmia kymmeniin ellei satoihin tietokoneisiin ja jatkaa leviämistään lukemattomiin tietokoneisiin ja tietoverkkoihin.

Tietoturvan ylläpito on nyt tärkeämpää kuin koskaan, vaarallisten haittaohjelmien leviämistapojen ja ominaisuuksien laajetessa yhä useampiin arkipäivän tietoverkkoa käyttäviin laitteistoihin, vaikuttaen jokaisen henkilökohtaisen tiedon tai omaisuuden menetykseen. Koskaan ei ole liian myöhäistä asentaa haittaohjelmista puhtaalle tietokoneelle uutta virustorjuntaohjelmistoa tai vaihtaa tärkeiden sähköpostiosoitteiden salasanaa. Kysymys kuuluukin pystyykö peruskäyttäjä ymmärtämään tekemänsä virheet tietoturvaa kohtaan ja miten hän kykenee ennaltaehkäisemään muiden henkilöiden tietoturvan laiminlyönnin seuraukset omassa tietoverkossaan. Selkeät ja yksinkertaiset ohjeet riittävät, mutta ilman vastuun noudattamista ohjeet ovat turhia. Ota siis askel eteenpäin kohti parempaa tietoturvaa kantamalla henkilökohtaisen vastuusi tietoverkkojen turvallisessa käytössä ja autat maailmanlaajuisen tietoturvan kehitystä omalla pienellä panoksellasi.

10 perusohjetta tietoverkkojen ja tietokoneen turvallisempaan käyttöön:

1. Asenna tietokoneellesi ja itsellesi sopiva virustorjuntaohjelmisto. Muista ylläpitää sitä ja käyttää automaattista päivitystä, virustorjuntaa sekä virustarkastusta.
2. Käytä tietoverkkoja tarvittavalla vastuulla ja pidä huolta omasta tietoturvasta tunnistamalla oman internetin käytön mahdolliset riskitekijät.
3. Pidä salasana suojassa muilta henkilöiltä, vaihda se usein sekä käytä erilaista salasanaa eri palveluissa ja tietokoneissa.
4. Pidä huolta palomuurin toiminnasta ja vältä avaamasta verkkoliikenteen portteja tietokoneen ohjelmistoille.
5. Käytä sähköpostipalveluita varoen, vältä avaamasta sähköpostiliitteitä ilman liitteen virustarkastusta ja avaa vain luotetuista lähteistä tulleita sähköposteja.
6. Tutustu haittaohjelmien toimintaan, jotta osaat tartuntavaiheessa tunnistaa haittaohjelman tyypin ja toimia tarvittavalla tavalla sen leviämisen ehkäisemiseksi ja poistamiseksi.
7. Älä lataa laittomia sekä tuntemattomista että epämääräisistä lähteistä saatavia tiedostoja. Vältä myös P2P- ohjelmien käyttöä tiedostojen latauksessa.
8. Käytä internetissä turvallista internetselainta ja muista päivittää internetselaimesi uusilla päivityksillä.
9. Päivitä Windows- käyttöjärjestelmäsi uusilla tietoturvapäivityksillä silloin kun niitä on saatavilla.
10. Vältä ohjelmistoja, jotka sisältävät vaarallisia tietoturva-aukkoja. Varmista asentaessa, että ohjelmisto on turvallinen käyttää.

LÄHTEET

Strickland, J. 2010. 10 worst computer viruses of all time. [WWW-dokumentti]. [Viitattu: 14.4.2010]. Saatavissa: http://computer.howstuffworks.com/worst-computer-viruses.htm

McAfee Labs. 2009. 2010 Threat Predictions. [WWW-dokumentti]. [Viitattu 8.3.2010]. Saatavissa: http://www.mcafee.com/us/local_content/ white_papers/7985rpt_labs_threat_predict_1209_v2.pdf

Reisinger, D. 16.6.2006. 25th anniversary of the computer virus? Not so fast. Cnet. [WWW-dokumentti]. [Viitattu 10.4.2010]. Saatavissa: http://news.cnet.com/8301-13506_3-9745010-17.html

Kivioja, P. 2009. C:\unknown.exe. Mikrobitti 12/2009, 35.

Computer hope. 2010. Computer virus information and help. [WWW-dokumentti]. [Viitattu 20.4.2010]. Saatavissa: http://www.computerhope.com/vlist.htm#02

About.com: Small Business: Canada. Brooks, T. Don't Be A Computer Virus Victim. [WWW-dokumentti]. [Viitattu 15.3.2010]. Saatavissa: http://sbinfocanada.about.com/cs/management/qt/avoidvirusts.htm

Emery, D. 16.1.2010. German government warns against using MS Explorer. BBC News. [WWW-dokumentti]. [Viitattu 20.4.2010]. Saatavissa: http://news.bbc.co.uk/2/hi/8463516.stm

Anti-trojan.org. Have I Got A Trojan? [WWW-dokumentti]. [Viitattu 8.3.2010]. Saatavissa: http://www.anti-trojan.org/haveigotatrojan.html

From, R., Lindfors, O. & Rönnholm, V. 12.12.2000. Henkilökohtaiset palomuurit. TTK. [WWW-dokumentti]. [Viitattu 22.3.2010]. Saatavissa:

http://www.netlab.tkk.fi/opetus/s38118/s00/tyot/44/palomuurit.shtml

Antivirus software pro. 5.1.2009. History of anti-virus software. [WWW-dokumentti]. [Viitattu 19.4.2010]. Saatavissa: http://www.antivirussoftwarepro.com/news/av-sw/history/

Virustorjunta.net. 26.1.2005. Hoax eli 'huijaus' – sähköpostiviesti. [WWW-dokumentti]. [Viitattu 9.3.2010]. Saatavissa: http://www.virustorjunta.net/modules.phpname=News&file=article&sid=485&mode=thread&order=0&thold=0

Brain, M. 2010. How Computer Viruses Work. Howstuffworks. [WWW-dokumentti]. [Viitattu 5.3.2010]. Saatavissa: http://computer.howstuffworks.com/computer-internet-security-channel.htm

Cuadra, F. 7.5.2003. How an antivirus program works. [WWW-dokumentti]. [Viitattu 15.4.2010]. Saatavissa: http://www.net-security.org/article.php?id=485&p=3

AntivirusWorld. 2009. How does anti-virus software work? [WWW-dokumentti]. [Viitattu 18.4.2010]. Saatavissa: http://www.antivirus-world.com/articles/antivirus.php

Microsoft. 22.3.2006. Hyvät salasanat: luominen ja käyttäminen. [WWW-dokumentti]. [Viitattu 3.3.2010]. Saatavissa: http://www.microsoft.com/finland/protect/yourself/password/create.mspx

Vance, A. 20.1.2010. If your password is 123456, just make it hackme. The New York Times. [WWW-dokumentti]. [Viitattu 14.4.2010]. Saatavissa: http://www.nytimes.com/2010/01/21/technology/21password.html

Pcguide. 2001. Major Virus Types and How They Work. [WWW-

dokumentti]. [Viitattu 16.4.2010]. Saatavissa: http://www.pcguide.com/care/data/virus/bgTypes-c.html

Kotilainen, S. 2010. Microsoft: turvattomat tietokoneet voisi eristää. Tietokone. [Verkkolehtijulkaisu]. [Viitattu 10.3.2010]. Saatavissa: http://www.tietokone.fi/uutiset/microsoft_turvattomat_tietokoneet_voisi_eristaa

Markus Jansson's Privacy And Security Page. Jansson, M. 2010. Mitä tehdä jos tietokoneesi hakkeroidaan tai se joutuu muunlaisen hyökkäyksen kohteeksi. [WWW-dokumentti]. [Viitattu 10.3.2010]. Saatavissa: http://www.markusjansson.net/fhacked.html#trojan

Lehto, T. 15.2.2010. Nordea torjuu verkkopankkihuijauksia tekstiviestivarmistuksella. Tietokone. [Verkkolehtijulkaisu]. [Viitattu 10.3.2010]. Saatavissa: http://www.tietokone.fi/uutiset/nordea_torjuu_verkkopankkihuijauksia_tekstiviestivarmistuksella

Karkimo, A. 8.4.2010. Opera paukutteli henkseleitään suotta. Tietokone. [Verkkolehtijulkaisu]. [Viitattu 21.4.2010]. Saatavissa: http://www.tietokone.fi/uutiset/firefoxin_suosio_laskee_syypaa_google

Viestintävirasto. 27.9.2007. Palomuuri [WWW-dokumentti]. [Viitattu 22.3.2010]. Saatavissa: http://www.ficora.fi/index/palvelut/palvelutai-heittain/tietoturva/palomuuri.html

Kotilainen, S. 15.3.2010. ”Rikolliset menevät kaiken virustorjunnan läpi”. Tietokone. [Verkkolehtijulkaisu]. [Viitattu 7.3.2010]. Saatavissa: http://www.tietokone.fi/uutiset/rikolliset_menevat_kaiken_virustorjunnan_lapi

Kotilainen, S. 17.2.2010. Rikollisten ykkösase: pdf-tiedosto. Tietokone. [Verkkolehtijulkaisu]. [Viitattu 8.3.2010]. Saatavissa: http://www.tietokone.fi/uutiset/rikollisten_ykkosase_pdf_tiedosto

Lehto, T. 27.1.2010. RSA: Verkkopankkien tietoturvaa voisi parantaa. Tietokone. [Verkkolehtijulkaisu]. [Viitattu 12.3.2010]. Saatavissa: http://www.tietokone.fi/uutiset/rsa_verkkopankkien_tietoturvaa_voisi _parantaa

Kautiala, J. 2004. Spyware eli vakoiluohjelmat. [Verkkojulkaisu]. Tampere: tietojenkäsittelytieteiden laitos. [Viitattu 2.3.2010]. Saatavissa: http://www.cs.uta.fi/reports/bsarja/B-2004-8.pdf

Symantec. 2010. Symantec global internet security threat report trends for 2009. [Verkkojulkaisu]. [Viitattu 21.4.2010]. Saatavissa: http://eval.symantec.com/mktginfo/enterprise/white_papers/bwhitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf

Karkimo, A. 9.3.2010. Sähköpostitilit huonossa suojassa. Tietokone. [Verkkolehtijulkaisu]. [Viitattu 15.3.2010]. Saatavissa: http://www.tietokone.fi/uutiset/sahkopostitilit_huonossa _suojassa

Karkimo, A. 25.1.2010. Tavis toivoo jonkun muun takaavan tietoturvansa. Tietokone. [Verkkolehtijulkaisu]. [Viitattu 15.3.2010]. Saatavissa: http://www.tietokone.fi/uutiset/tavis_toivoo_jonkun_muun_takaavan_tietoturvansa

Resick, N. 12.3.2010. The evolution of the computer virus into antivirus xp 2009, the worst virus ever. Free Press Release. [WWW-dokumentti]. [Viitattu 10.4.2010]. Saatavissa: http://www.free-press-release.com/news-the-evolution-of-the-computer-virus-into-antivirus-xp-2009-the-worst-virus-ever-1268439473.html

Sapronov, K. 2005. The human factor and information security. [WWW-dokumentti]. [Viitattu: 14.4.2010]. Saatavissa: http://www.securelist.com/en/analysis/176195190/The_human_factor_and_information_security

Kuivanen, I. 2003. Tiedostovirukset. [WWW-dokumentti]. [Viitattu 11.03.2010]. Saatavissa: http://cs.stadia.fi/~kuivanen/tietoturva/tiedosto.html

Tampereen yliopisto. 2009. Tietokonekeskus – IT-tietoturva. [WWW-dokumentti]. [Viitattu 5.3.2010]. Saatavissa: http://www.uta.fi/laitokset/tkk/tietoturva/index.html

Helenius, M. 2004. Tietokoneviruksista. Tampere: TIETOJENKÄSITTELYTIETEIDEN LAITOS. [Verkkojulkaisu]. [Viitattu 2.3.2010]. Saatavissa: http://*www.cs.uta.fi/reports/bsarja/B-2004-8.pdf*

Norton from symantec. 1.8.2006. Tietoja erilaisista virustyypeistä. [WWW-dokumentti]. [Viitattu 17.3.2010]. Saatavissa: http://www.symantec.com/fi/fi/norton/library/article.jsp?aid=article2_08_06

Cert-fi. 15.5.2007. Tietoturva nyt! Palvelunestohyökkäykset seurannassa. [WWW-dokumentti]. [Viitattu 22.4.2010]. Saatavissa: http://www.cert.fi/tietoturvanyt/2007/05/P_6.html

Cert-fi. 31.5.2007. Tietoturva nyt! Palvelunestohyökkäyksiä on monta lajia. [WWW-dokumentti]. [Viitattu 22.4.2010]. Saatavissa: http://www.cert.fi/tietoturvanyt/2007/05/P_12.html

Tietoturvakoulu. 26.11.2008. Tietoturvapäivä. [WWW-dokumentti]. [Viitattu 14.4.2010]. Saatavissa: http://www.tietoturvakoulu.fi/opettajille/tietoturvapaiva.html

Rosendahl, M. Tietoturva kuuluu kaikille. [WWW-dokumentti]. [Viitattu 12.3.2010]. Saatavissa: http://www.helsinki.fi/atk/lehdet/402/Tietoturva_kuuluu_kaikille.html

Tietoturvan historia ja tausta. Kajaanin Ammattikorkeakoulu [Verkkojulkaisu]. [Viitattu 17.3.2010]. Saatavissa: gallia.kajak.fi/.../Tietoturva/Historiaa%20ja%20taustaa.pdf

Viestintävirasto. 19.01.2010. Tietoturvapäivä 2010 lähestyy – laita päivä kalenteriin! [WWW-dokumentti]. [Viitattu 3.3.2010]. Saatavissa: http://www.ficora.fi/index/viestintavirasto/lehdistotiedotteet/2010/P_1.html

SpywareRemove. 05.02.2010. Top 10 Trojans from recent malware detections. [WWW-dokumentti]. [Viitattu: 24.3.2010] Saatavissa: http://www.spywareremove.com/security/top-10-trojans-malware-detections/

Read, J. Trojan Removal. [WWW-dokumentti]. Anti-trojan.org. [Viitattu 8.3.2010]. Saatavissa: http://www.anti-trojan.org/trojanremoval.html

TopBits.com. 2010. Trojan Virus. [WWW-dokumentti]. [Viitattu 8.3.2010]. Saatavissa: http://www.topbits.com/trojan-virus.html

Wells, J. IBM Research. 1996. Virustimeline. [WWW-dokumentti]. [Viitattu 17.3.2010]. Saatavissa: http://www.research.ibm.com/antivirus/timeline.htm

Pcsecurityalert.com. What are computer viruses? [WWW-dokumentti]. [Viitattu 16.4.2010]. Saatavissa: http://www.pcsecurityalert.com/pcsecurityalert-articles/what-is-a-computer-virus.htm